(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2005-286959
(P2005-286959A)
(43)公開日　平成17年10月13日(2005.10.13)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| H04L 9/08 | H04L 9/00 | 601B | 5B017 |
| G06F 12/14 | G06F 12/14 | 530C | 5J104 |
| | G06F 12/14 | 530P | |
| | G06F 12/14 | 540C | |
| | H04L 9/00 | 601E | |

審査請求 未請求　請求項の数 43　ＯＬ　（全 65 頁）

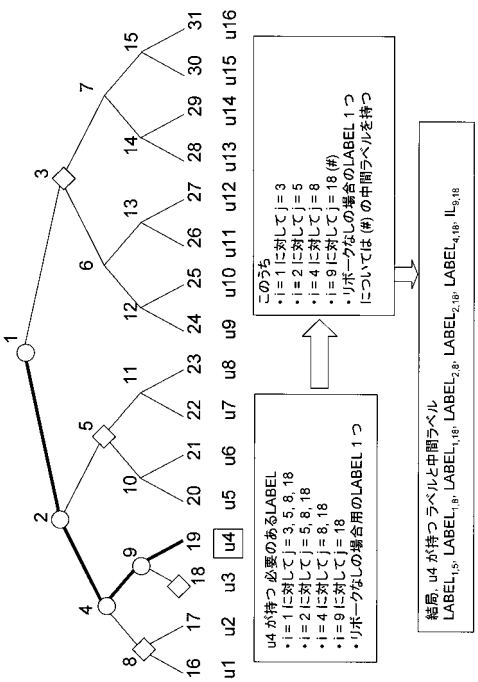
(21)出願番号　特願2004-102039 (P2004-102039)
(22)出願日　平成16年3月31日 (2004.3.31)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100093241
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

Ｆターム(参考)　5B017 AA03　BA07　BB10　CA16
5J104 AA16　EA17　EA18

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

(57)【要約】
【課題】　ＳＤ方式に基づく木構造を適用した暗号文提供構成において、暗号文復号を行なう機器に格納すべき情報量を削減可能とした構成を提供する。
【解決手段】　ＳＤ方式やＬＳＤ方式に基づいて設定するサブセット各々に対応するラベル中、特別サブセット対応のラベルを演算により算出可能とした中間ラベルを設定し、１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルを算出可能とした。受信機は、特別サブセット非対応のラベルと１つの中間ラベルを提供する。受信機は保持する中間ラベルに対する落とし戸つき一方向性置換Ｆの実行により他の中間ラベルを算出し、全ての必要なラベルを算出できる。
【選択図】　図１９



【特許請求の範囲】
【請求項１】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成する情報処理方法であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成ステップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定するステップであり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定ステップと、
を有することを特徴とする情報処理方法。
【請求項２】
前記情報処理方法は、さらに、
前記ラベル生成ステップにおいて生成したサブセット対応の各ラベルから導出されるサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成し、前記受信機に提供する暗号文生成ステップを有することを特徴とする請求項１に記載の情報処理方法。
【請求項３】
前記ラベル生成ステップは、
中間ラベルに対するハッシュ算出処理により、特別サブセットに対応するラベルの値を算出するステップを含むことを特徴とする請求項１に記載の情報処理方法。
【請求項４】
前記ラベル生成ステップは、
特別サブセットに対応するラベルの値に対する擬似乱数生成処理により、他のラベルを生成するステップを含むことを特徴とする請求項１に記載の情報処理方法。
【請求項５】
前記中間ラベル生成ステップは、
ノード数２Ｎ－１の階層木において、値$x_1 \in Z^*_M$をランダムに選択し、ｉをカウンタとして、ｉ＝２～２Ｎ－１までｉを１つずつ増加させながら、落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式である下記式、
【数１】

$$x_i = (x_{\lfloor i/2 \rfloor} + i)^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

または、下記式、

【数２】

$$x_i = (x_{\lfloor i/2 \rfloor} + h(i))^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

ただし、Ｍ、ｄは、暗号パラメータとしての法Ｍおよび秘密指数ｄ、

上記式のいずれかを適用して、ノード数２Ｎ－１の階層木におけるノード対応値$x_1$～$x_{2N-1}$を算出し、これを、特別サブセット対応ラベルを算出可能な中間ラベル（ＩＬ）の値として設定するステップであることを特徴とする請求項１に記載の情報処理方法。

【請求項６】

前記中間ラベル生成ステップにおいて選択する特別サブセットは、

階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、

階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、

の少なくともいずれかであることを特徴とする請求項１に記載の情報処理方法。

【請求項７】

前記提供ラベル決定ステップは、

前記階層木の末端ノード対応の受信機に提供する１つの中間ラベルを前記第１特別サブセットを構成するサブセット$S_{i,j}$中、最下層のサブセットに対応する中間ラベルとするステップであることを特徴とする請求項１に記載の情報処理方法。

【請求項８】

前記中間ラベル生成ステップは、

階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする請求項１乃至７いずれかに記載の情報処理方法。

【請求項９】

前記中間ラベル生成ステップは、

階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする請求項１乃至７いずれかに記載の情報処理方法。

【請求項１０】

階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する復号処理方法であり、

前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択ステップと、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出ステップと、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するステップと、
生成サブセットキーを適用して暗号文の復号処理を実行する復号ステップと、
を有することを特徴とする復号処理方法。

【請求項１１】
前記ラベル算出ステップは、
保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より他の中間ラベルを算出するステップを含むことを特徴とする請求項１０に記載の復号処理方法。

【請求項１２】
前記ラベル算出ステップは、
保持中間ラベル、または、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より算出した他の中間ラベルに対するハッシュ演算によるラベル算出を実行するステップを含むことを特徴とする請求項１０に記載の復号処理方法。

【請求項１３】
前記ラベル算出ステップは、
暗号文の適用サブセットキーが、
階層木においてノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセット、または、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセット、
のいずれかの特別サブセット対応のラベルに基づく擬似乱数生成処理により算出可能なサブセットキーであり、前記特別サブセット対応のラベルを保持していない場合に、保持している中間ラベルに対する演算処理により前記特別サブセット対応のラベルを算出するステップであることを特徴とする請求項１０に記載の復号処理方法。

【請求項１４】
前記ラベル算出ステップは、
前記階層木において、復号処理を実行する受信機の設定ノードからルートに至るパス上のノードを包含する特別サブセットに対応するラベルの算出を保持中間ラベルに対する演算処理により算出するステップであることを特徴とする請求項１０に記載の復号処理方法。

【請求項１５】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行する情報処理方法であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成ステップを有し、
暗号文生成ステップにおいて適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とする情報処理方法。

【請求項１６】

前記情報処理方法は、さらに、
サブセットキーを生成するサブセットキー生成ステップを有し、
前記サブセットキー生成ステップは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）に基づく擬似乱数生成処理によりサブセットキーを生成する処理であ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１７】
前記情報処理方法は、さらに、
サブセットキーを生成するサブセットキー生成ステップを有し、
前記サブセットキー生成ステップは、
値$x_1 \in Z^*_M$と、暗号パラメータとしての法Ｍおよび秘密指数ｄとを適用した落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式に基づいて、前記特別サブセットに対応する中間ラベルを生成する中間ラベル生成ステップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記ラベルに基づく演算処理によりサブセットキーを算出するステップと、
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１８】
前記中間ラベル生成ステップにおいて選択する特別サブセットは、
階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、
階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、
の少なくともいずれかであることを特徴とする請求項１７に記載の情報処理方法。
【請求項１９】
前記中間ラベル生成ステップは、
階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする請求項１８に記載の情報処理方法。
【請求項２０】
前記中間ラベル生成ステップは、
階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする請求項１８に記載の情報処理方法。
【請求項２１】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成する情報処理装置であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成手段と、

前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成手段と、

前記階層木の末端ノード対応の受信機に対する提供ラベルを決定する提供ラベル決定手段であり、

前記特別サブセットに対応しない特別サブセット非対応ラベルと、

演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、

を受信機に対する提供ラベルとして決定する提供ラベル決定手段と、

を有することを特徴とする情報処理装置。

【請求項２２】

前記情報処理装置は、さらに、

前記ラベル生成手段において生成したサブセット対応の各ラベルから導出されるサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成し、前記受信機に提供する暗号文生成手段を有することを特徴とする請求項２１に記載の情報処理装置。

【請求項２３】

前記ラベル生成手段は、

中間ラベルに対するハッシュ算出処理により、特別サブセットに対応するラベルの値を算出する構成であることを特徴とする請求項２１に記載の情報処理装置。

【請求項２４】

前記ラベル生成手段は、

特別サブセットに対応するラベルの値に対する擬似乱数生成処理により、他のラベルを生成する構成であることを特徴とする請求項２１に記載の情報処理装置。

【請求項２５】

前記中間ラベル生成手段は、

ノード数２Ｎ－１の階層木において、値$x_1 \in Z^*_M$をランダムに選択し、ｉをカウンタとして、ｉ＝２～２Ｎ－１までｉを１つずつ増加させながら、落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式である下記式、

【数３】

$$x_i = (x_{\lfloor i/2 \rfloor} + i)^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

または、下記式、

【数４】

$$x_i = (x_{\lfloor i/2 \rfloor} + h(i))^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

ただし、Ｍ、ｄは、暗号パラメータとしての法Ｍおよび秘密指数ｄ、

上記式のいずれかを適用して、ノード数２Ｎ－１の階層木におけるノード対応値$x_1$～$x_{2N-1}$を算出し、これを、特別サブセット対応ラベルを算出可能な中間ラベル（ＩＬ）の値として設定する構成であることを特徴とする請求項２１に記載の情報処理装置。

【請求項２６】

前記中間ラベル生成手段において選択する特別サブセットは、

階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、

階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、

の少なくともいずれかであることを特徴とする請求項１５に記載の情報処理装置。

【請求項２７】

前記提供ラベル決定手段は、

前記階層木の末端ノード対応の受信機に提供する１つの中間ラベルを前記第１特別サブセットを構成するサブセット$S_{i,j}$中、最下層のサブセットに対応する中間ラベルとすることを特徴とする請求項２１に記載の情報処理装置。

【請求項２８】

前記中間ラベル生成手段は、

階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定する手段であることを特徴とする請求項２１乃至２７いずれかに記載の情報処理装置。

【請求項２９】

前記中間ラベル生成手段は、

階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定する手段であることを特徴とする請求項２１乃至２７いずれかに記載の情報処理装置。

【請求項３０】

階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する情報処理装置であり、

前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可

能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択手段と、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出手段と、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するサブセットキー生成手段と、
生成サブセットキーを適用して暗号文の復号処理を実行する復号手段と、
を有することを特徴とする情報処理装置。

【請求項３１】
前記ラベル算出手段は、
保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より他の中間ラベルを算出する構成であることを特徴とする請求項３０に記載の情報処理装置。

【請求項３２】
前記ラベル算出手段は、
保持中間ラベル、または、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より算出した他の中間ラベルに対するハッシュ演算によるラベル算出を実行する構成であることを特徴とする請求項３０に記載の情報処理装置。

【請求項３３】
前記ラベル算出手段は、
暗号文の適用サブセットキーが、
階層木においてノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセット、または、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセット、
のいずれかの特別サブセット対応のラベルに基づく擬似乱数生成処理により算出可能なサブセットキーであり、前記特別サブセット対応のラベルを保持していない場合に、保持している中間ラベルに対する演算処理により前記特別サブセット対応のラベルを算出する構成であることを特徴とする請求項３０に記載の情報処理装置。

【請求項３４】
前記ラベル算出手段は、
前記階層木において、復号処理を実行する受信機の設定ノードからルートに至るパス上のノードを包含する特別サブセットに対応するラベルの算出を保持中間ラベルに対する演算処理により算出する構成であることを特徴とする請求項３０に記載の情報処理装置。

【請求項３５】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行する情報処理装置であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成手段を有し、
暗号文生成手段において適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とする情報処理装置。

【請求項３６】
前記情報処理装置は、さらに、
サブセットキーを生成するサブセットキー生成手段を有し、

前記サブセットキー生成手段は、
サブセット各々に対応するラベル（ＬＡＢＥＬ）に基づく擬似乱数生成処理によりサブセットキーを生成する構成であることを特徴とする請求項３５に記載の情報処理装置。
【請求項３７】
前記情報処理装置は、さらに、
サブセットキーを生成するサブセットキー生成手段を有し、
前記サブセットキー生成手段は、
値$x_1 \in Z^*_M$と、暗号パラメータとしての法Ｍおよび秘密指数ｄとを適用した落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式に基づいて、前記特別サブセットに対応する中間ラベルを生成し、前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成し、生成ラベルに基づく演算処理によりサブセットキーを算出する構成であることを特徴とする請求項３５に記載の情報処理装置。
【請求項３８】
前記特別サブセットは、
階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、
階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、
の少なくともいずれかであることを特徴とする請求項３５に記載の情報処理装置。
【請求項３９】
前記サブセットは、階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセットであることを特徴とする請求項３５に記載の情報処理装置。
【請求項４０】
前記サブセットは、階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセットであることを特徴とする請求項３５に記載の情報処理装置。
【請求項４１】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成するコンピュータ・プログラムであり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成ステップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定するステップであり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定ステップと、
を有することを特徴とするコンピュータ・プログラム。

【請求項４２】
階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行するコンピュータ・プログラムであり、
前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択ステップと、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出ステップと、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するステップと、
生成サブセットキーを適用して暗号文の復号処理を実行する復号ステップと、
を有することを特徴とするコンピュータ・プログラム。
【請求項４３】
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行するコンピュータ・プログラムであり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成ステップを有し、
暗号文生成ステップにおいて適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であ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】
本発明は、情報処理方法、復号処理方法、および情報処理装置、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、階層木構造を適用したブロードキャストエンクリプション方式において現在知られているＳｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式、およびＬａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（ＬＳＤ）方式において、受信機が安全に保持する必要のあるラベルなどの秘密情報の量を削減し効率的でセキュアな情報配信を実現する情報処理方法、復号処理方法、および情報処理装置、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、様々なソフトウエアデータ（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ＣＤ(Compact Disc)、ＤＶＤ(Digital Versatile Disk)、ＭＤ(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ＰＣ（Personal Computer）やプレーヤ、あるいはゲーム機器等、様々な情報処理装置において再生され利用される。
【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。

【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、ＣＤ－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。

【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、その最下層がリーフ（葉）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。

【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。

【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。

【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ＮＫｎ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。

【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。

【００１６】

上述のブロードキャストエンクリプション（Broadcast Encryption）方式は、Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ方式と呼ばれる。このような木構造を用いて情報配信を行なう場合、リーフに対応する情報処理装置（ユーザ機器）が増大すると同報送信すべきメッセージが増大し、また各情報処理装置（ユーザ機器）において安全に格納すべきノードキーなどの鍵情報も増大してしまうという問題がある。

【００１７】

このような問題を解決する手法として、これまでに提案されている方式として、Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式、および、その改良版であるＬａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＬＳＤ）方式がある。ＳＤ方式については、例えば非特許文献１に記載され、ＬＳＤ方式については、例えば非特許文献２に記載されている。

【００１８】

いずれの方式も、ブロードキャストエンクリプションシステムの全受信機（受信者）数をＮとし、そのうち排除（リボーク）される、即ち、同報通信される秘密情報を受け取ることができない受信機の数をｒとしたときに、同報通信すべきメッセージ（暗号文）の数がＯ（ｒ）であり、これは上述したＣｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ方式などの他方式に比べて小さく、優れている。

【００１９】

しかし、各受信機が安全なメモリに保持すべき鍵（ラベル）の数が、ＳＤ方式では$O(\log^2 N)$、ＬＳＤ方式では、$O(\log^{1+\varepsilon} N)$となる。ここでεは任意の正の数である。この鍵の数は、Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ方式などの他方式に比べて多く、これを減らすことが課題となっている。なお、本明細書においては、特に断りのない限りｌｏｇの底は２である。

【非特許文献１】Ａｄｖａｎｃｅｓ　ｉｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ－Ｃｒｙｐｔｏ２００１，Ｌｅｃｔｕｒｅ　Ｎｏｔｅｓ　ｉｎ　Ｃｏｍｐｕｔｅｒ　Ｓｃｉｅｎｃｅ２１３９，Ｓｐｒｉｎｇｅｒ，２００１　ｐｐ．４１－６２「Ｄ．Ｎａｏｒ，Ｍ．Ｎａｏｒ　ａｎｄ　Ｊ．Ｌｏｔｓｐｉｅｃｈ著"Ｒｅｖｏｃａｔｉｏｎ　ａｎｄ　Ｔｒａｃｉｎ

g Schemes for Stateless Receivers"」
【非特許文献２】Advances in Cryptography－Crypto 2002, Lecture Notes in Computer Science 2442, Springer, 2002, pp47－60「D. Halevy and A. Shamir著"The LSD Broadcast Encryption Scheme"」
【発明の開示】
【発明が解決しようとする課題】
【００２０】
本発明は、このような状況に鑑みてなされたものであり、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情報配信構成において比較的に効率的な構成であるとされているＳｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式、およびＬａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（ＬＳＤ）方式に対して、以下において説明する１つの落とし戸つき一方向性置換に基づく一方向性置換木を適用することにより受信機が安全に保持する必要のあるラベルなどの秘密情報の量を削減し効率的でセキュアな情報配信を実現する情報処理方法、復号処理方法、および情報処理装置、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】
【００２１】
本発明の第１の側面は、
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成する情報処理方法であり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成ステップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定するステップであり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定ステップと、
を有することを特徴とする情報処理方法にある。
【００２２】
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、さらに、前記ラベル生成ステップにおいて生成したサブセット対応の各ラベルから導出されるサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成し、前記受信機に提供する暗号文生成ステップを有することを特徴とする。
【００２３】
さらに、本発明の情報処理方法の一実施態様において、前記ラベル生成ステップは、中間ラベルに対するハッシュ算出処理により、特別サブセットに対応するラベルの値を算出するステップを含むことを特徴とする。
【００２４】
さらに、本発明の情報処理方法の一実施態様において、前記ラベル生成ステップは、特別サブセットに対応するラベルの値に対する擬似乱数生成処理により、他のラベルを生成するステップを含むことを特徴とする。

【００２５】
さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップは、ノード数２Ｎ－１の階層木において、値$x_1 \in Z^*_M$をランダムに選択し、ｉをカウンタとして、ｉ＝２～２Ｎ－１までｉを１つずつ増加させながら、落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式である下記式、
【数５】

$$x_i = (x_{\lfloor i/2 \rfloor} + i)^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

または、下記式、
【数６】

$$x_i = (x_{\lfloor i/2 \rfloor} + h(i))^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

ただし、Ｍ、ｄは、暗号パラメータとしての法Ｍおよび秘密指数ｄ、
上記式のいずれかを適用して、ノード数２Ｎ－１の階層木におけるノード対応値$x_1$～$x_{2N-1}$を算出し、これを、特別サブセット対応ラベルを算出可能な中間ラベル（ＩＬ）の値として設定するステップであることを特徴とする。
【００２６】
さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップにおいて選択する特別サブセットは、階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、の少なくともいずれかであることを特徴とする。
【００２７】
さらに、本発明の情報処理方法の一実施態様において、前記提供ラベル決定ステップは、前記階層木の末端ノード対応の受信機に提供する１つの中間ラベルを前記第１特別サブセットを構成するサブセット$S_{i,j}$中、最下層のサブセットに対応する中間ラベルとするステップであることを特徴とする。
【００２８】
さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップは

、階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする。

【００２９】

さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップは、階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする。

【００３０】

さらに、本発明の第２の側面は、

階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する復号処理方法であり、

前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択ステップと、

暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出ステップと、

保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するステップと、

生成サブセットキーを適用して暗号文の復号処理を実行する復号ステップと、

を有することを特徴とする復号処理方法にある。

【００３１】

さらに、本発明の復号処理方法の一実施態様において、前記ラベル算出ステップは、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より他の中間ラベルを算出するステップを含むことを特徴とする。

【００３２】

さらに、本発明の復号処理方法の一実施態様において、前記ラベル算出ステップは、保持中間ラベル、または、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より算出した他の中間ラベルに対するハッシュ演算によるラベル算出を実行するステップを含むことを特徴とする。

【００３３】

さらに、本発明の復号処理方法の一実施態様において、前記ラベル算出ステップは、暗号文の適用サブセットキーが、階層木においてノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセット、または、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセット、のいずれかの特別サブセット対応のラベルに基づく擬似乱数生成処理により算出可能なサブセットキーであり、前記特別サブセット対応のラベルを保持していない場合に、保持している中間ラベルに対する演算処理により前記特別サブセット対応のラベルを算出するステップであることを特徴とする。

【００３４】

さらに、本発明の復号処理方法の一実施態様において、前記ラベル算出ステップは、前記階層木において、復号処理を実行する受信機の設定ノードからルートに至るパス上のノ

ードを包含する特別サブセットに対応するラベルの算出を保持中間ラベルに対する演算処理により算出するステップであることを特徴とする。

【００３５】

さらに、本発明の第３の側面は、

階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行する情報処理方法であり、

階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成ステップを有し、

暗号文生成ステップにおいて適用するサブセットキーは、

サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とする情報処理方法にある。

【００３６】

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、さらに、サブセットキーを生成するサブセットキー生成ステップを有し、前記サブセットキー生成ステップは、サブセット各々に対応するラベル（ＬＡＢＥＬ）に基づく擬似乱数生成処理によりサブセットキーを生成する処理であることを特徴とする。

【００３７】

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、さらに、サブセットキーを生成するサブセットキー生成ステップを有し、前記サブセットキー生成ステップは、値$x_1 \in Z^*_M$と、暗号パラメータとしての法Ｍおよび秘密指数ｄとを適用した落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式に基づいて、前記特別サブセットに対応する中間ラベルを生成する中間ラベル生成ステップと、前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、前記ラベルに基づく演算処理によりサブセットキーを算出するステップとを含むことを特徴とする。

【００３８】

さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップにおいて選択する特別サブセットは、階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットとの少なくともいずれかであることを特徴とする。

【００３９】

さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップは、階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする。

【００４０】

さらに、本発明の情報処理方法の一実施態様において、前記中間ラベル生成ステップは、階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択

された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定するステップであることを特徴とする。

【００４１】

さらに、本発明の第４の側面は、

階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成する情報処理装置であり、

階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成手段と、

前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成手段と、

前記階層木の末端ノード対応の受信機に対する提供ラベルを決定する提供ラベル決定手段であり、

前記特別サブセットに対応しない特別サブセット非対応ラベルと、

演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、

を受信機に対する提供ラベルとして決定する提供ラベル決定手段と、

を有することを特徴とする情報処理装置にある。

【００４２】

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、さらに、前記ラベル生成手段において生成したサブセット対応の各ラベルから導出されるサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成し、前記受信機に提供する暗号文生成手段を有することを特徴とする。

【００４３】

さらに、本発明の情報処理装置の一実施態様において、前記ラベル生成手段は、中間ラベルに対するハッシュ算出処理により、特別サブセットに対応するラベルの値を算出する構成であることを特徴とする。

【００４４】

さらに、本発明の情報処理装置の一実施態様において、前記ラベル生成手段は、特別サブセットに対応するラベルの値に対する擬似乱数生成処理により、他のラベルを生成する構成であることを特徴とする。

【００４５】

さらに、本発明の情報処理装置の一実施態様において、前記中間ラベル生成手段は、ノード数２Ｎ－１の階層木において、値$x_1 \in Z^*_M$をランダムに選択し、ｉをカウンタとして、ｉ＝２～２Ｎ－１までｉを１つずつ増加させながら、落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式である下記式、

【数７】

$$x_i = (x_{\lfloor i/2 \rfloor} + i)^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

または、下記式、

【数８】

$$x_i = (x_{\lfloor i/2 \rfloor} + h(i))^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

ただし、Ｍ、ｄは、暗号パラメータとしての法Ｍおよび秘密指数ｄ、

上記式のいずれかを適用して、ノード数２Ｎ－１の階層木におけるノード対応値$x_1$～$x_{2N-1}$を算出し、これを、特別サブセット対応ラベルを算出可能な中間ラベル（ＩＬ）の値として設定する構成であることを特徴とする。

【００４６】

さらに、本発明の情報処理装置の一実施態様において、前記中間ラベル生成手段において選択する特別サブセットは、階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、の少なくともいずれかであることを特徴とする。

【００４７】

さらに、本発明の情報処理装置の一実施態様において、前記提供ラベル決定手段は、前記階層木の末端ノード対応の受信機に提供する１つの中間ラベルを前記第１特別サブセットを構成するサブセット$S_{i,j}$中、最下層のサブセットに対応する中間ラベルとすることを特徴とする。

【００４８】

さらに、本発明の情報処理装置の一実施態様において、前記中間ラベル生成手段は、階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定する手段であることを特徴とする。

【００４９】
さらに、本発明の情報処理装置の一実施態様において、前記中間ラベル生成手段は、階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルを、該特別サブセット対応の中間ラベル（ＩＬ）から算出可能な値として設定する手段であることを特徴とする。
【００５０】
さらに、本発明の第５の側面は、
階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する情報処理装置であり、
前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択手段と、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出手段と、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するサブセットキー生成手段と、
生成サブセットキーを適用して暗号文の復号処理を実行する復号手段と、
を有することを特徴とする情報処理装置にある。
【００５１】
さらに、本発明の情報処理装置の一実施態様において、前記ラベル算出手段は、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より他の中間ラベルを算出する構成であることを特徴とする。
【００５２】
さらに、本発明の情報処理装置の一実施態様において、前記ラベル算出手段は、保持中間ラベル、または、保持中間ラベルに対する落とし戸つき一方向性置換Ｆの実行より算出した他の中間ラベルに対するハッシュ演算によるラベル算出を実行する構成であることを特徴とする。
【００５３】
さらに、本発明の情報処理装置の一実施態様において、前記ラベル算出手段は、暗号文の適用サブセットキーが、階層木においてノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセット、または、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセット、のいずれかの特別サブセット対応のラベルに基づく擬似乱数生成処理により算出可能なサブセットキーであり、前記特別サブセット対応のラベルを保持していない場合に、保持している中間ラベルに対する演算処理により前記特別サブセット対応のラベルを算出する構成であることを特徴とする。
【００５４】
さらに、本発明の情報処理装置の一実施態様において、前記ラベル算出手段は、前記階層木において、復号処理を実行する受信機の設定ノードからルートに至るパス上のノードを包含する特別サブセットに対応するラベルの算出を保持中間ラベルに対する演算処理により算出する構成であることを特徴とする。
【００５５】
さらに、本発明の第６の側面は、
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行する情報処理装置であり、

階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成手段を有し、

暗号文生成手段において適用するサブセットキーは、

サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とする情報処理装置にある。

【００５６】

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、さらに、サブセットキーを生成するサブセットキー生成手段を有し、前記サブセットキー生成手段は、サブセット各々に対応するラベル（ＬＡＢＥＬ）に基づく擬似乱数生成処理によりサブセットキーを生成する構成であることを特徴とする。

【００５７】

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、さらに、サブセットキーを生成するサブセットキー生成手段を有し、前記サブセットキー生成手段は、値$x_1 \in Z^*_M$と、暗号パラメータとしての法Ｍおよび秘密指数ｄとを適用した落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式に基づいて、前記特別サブセットに対応する中間ラベルを生成し、前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成し、生成ラベルに基づく演算処理によりサブセットキーを算出する構成であることを特徴とする。

【００５８】

さらに、本発明の情報処理装置の一実施態様において、前記特別サブセットは、階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、の少なくともいずれかであることを特徴とする。

【００５９】

さらに、本発明の情報処理装置の一実施態様において、前記サブセットは、階層木中に設定した１つの特別レベルによって分離したレイヤ別のサブセット管理構成を持つベーシックＬＳＤ（Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセットであることを特徴とする。

【００６０】

さらに、本発明の情報処理装置の一実施態様において、前記サブセットは、階層木中に設定した複数の特別レベルによって分離したレイヤ別のサブセット管理構成を持つ一般化ＬＳＤ（Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に従って設定するサブセットであることを特徴とする。

【００６１】

さらに、本発明の第７の側面は、

階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の提供処理に適用する階層木を生成するコンピュータ・プログラムであり、

階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）であり、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ中間ラベルを生成する中間ラベル生成ステ

ップと、
前記中間ラベルに基づく演算処理により、前記特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成ステップと、
前記階層木の末端ノード対応の受信機に対する提供ラベルを決定するステップであり、
前記特別サブセットに対応しない特別サブセット非対応ラベルと、
演算処理によって前記特別サブセットに対応するラベルを算出可能とした中間ラベルと、
を受信機に対する提供ラベルとして決定する提供ラベル決定ステップと、
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。

【００６２】
さらに、本発明の第８の側面は、
階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行するコンピュータ・プログラムであり、
前記暗号文から、自己の保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する暗号文選択ステップと、
暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、保持中間ラベルに対する演算処理を実行して特別サブセット対応のラベルを算出するラベル算出ステップと、
保持ラベルまたは算出ラベルに基づく擬似乱数生成処理によってサブセットキーを生成するステップと、
生成サブセットキーを適用して暗号文の復号処理を実行する復号ステップと、
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。

【００６３】
さらに、本発明の第９の側面は、
階層木構成に基づくブロードキャストエンクリプション方式により特定選択機器のみの復号を可能とした暗号文の生成処理を実行するコンピュータ・プログラムであり、
階層木を適用したＳＤ（Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する暗号文生成ステップを有し、
暗号文生成ステップにおいて適用するサブセットキーは、
サブセット各々に対応するラベル（ＬＡＢＥＬ）から算出可能なサブセットキーであり、選択された一部の特別サブセットに対応するラベルの値が、中間ラベル（ＩＬ）に基づく演算処理により算出可能であり、前記中間ラベルは、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な設定であることを特徴とするコンピュータ・プログラムにある。

【００６４】
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。

【００６５】
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】

【００６６】

本発明の構成によれば、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情報配信構成において比較的に効率的な構成であるとされているＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式、およびＬａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＬＳＤ）方式に対して、さらに１つの落とし戸つき一方向性置換に基づく一方向性置換木を適用することにより、各受信機（情報処理装置）が安全に保持すべき情報量を削減することが可能となる。

【００６７】

さらに、本発明の構成においては、ＳＤ方式やＬＳＤ方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）を生成し、この中間ラベルについて、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ構成とした。受信機には、特別サブセット非対応のラベルに加えて、特別サブセット対応のラベルを導出可能な１つの中間ラベルのみを提供する構成としたので、従来のＳＤ方式やＬＳＤ方式において受信機に提供されるラベルの数を、削減することが可能となる。削減したラベルについては、受信機側で保持する中間ラベルに対する落とし戸つき一方向性置換Ｆの実行により他の中間ラベルを算出可能であり、従来のＳＤ方式やＬＳＤ方式に基づいて設定可能なサブセットの全てに対応する処理が可能である。このように本発明の構成を適用することにより、各受信機が安全に保持すべき情報量（ラベル）の削減が実現する。

【発明を実施するための最良の形態】

【００６８】

以下、図面を参照しながら本発明の情報処理方法、復号処理方法、および情報処理装置、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。

【００６９】

なお、説明は、以下の項目に従って行なう。

１．Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式の概要

２．Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式の概要

３．一方向性置換木を用いたＳＤ方式のラベル数削減構成

４．一方向性置換木の構成方法例

５．一方向性置換木を適用した情報配信処理例

６．Ｂａｓｉｃ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ベーシックＬＳＤ）方式の概要

７．一方向性置換木を用いたベーシックＬＳＤ方式のラベル数削減構成

８．Ｇｅｎｅｒａｌ　Ｌａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（一般化ＬＳＤ）方式の概要

９．一方向性置換木を用いた一般化ＬＳＤ方式のラベル数削減構成

【００７０】

［１．Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式の概要］

まず既存の階層型木構造を適用したブロードキャストエンクリプション（Broadcast Encryption）方式として知られているＣｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式の概要について説明する。

【００７１】

なお、以下の説明においては、簡単のために、階層型木構造のリーフに対応して設定される情報処理装置（受信機）の総数Ｎは２のべき乗の数であるとする。また、以下の説明において、関数ｌｏｇの底はすべて２である。なお、階層型木構造のリーフに対応する機器は、以下に説明する秘密情報の復号処理を実行可能であれば、様々な機器、例えばＰＣ、携帯端末など、様々な情報処理装置の設定が可能である。ここでは、これらを総称して

受信機として説明する。また、本発明における暗号文配信処理とは、通信ネットワークを介した通信による提供処理のみならず、記録媒体に格納した暗号文の提供処理も含むものである。

【００７２】

なお、以下の説明においては、下記の記号を用いて説明する。

Ｐ（ｉ）：ノードｉの親ノードおよびそのノード番号

Ｓ（ｉ）：ノードｉの兄弟（ｓｉｂｌｉｎｇ）であるノード（すなわち、ｉと異なるノードで、ｉと同じ親を持つノード）およびそのノード番号

ＬＣ（ｉ）：ノードｉの左側の子ノードおよびそのノード番号

ＲＣ（ｉ）：ノードｉの右側の子ノードおよびそのノード番号

【００７３】

（１）Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式

Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式は、基本的に背景技術の欄において説明した構成に相当し、図３に示すように、階層型木構造として各ノードが２つに分岐する形を持つ２分木を用いる。図３は、受信機数Ｎ＝１６の例である。この２分木の各リーフ（葉）に各受信機を割り当てる（図３におけるｕ１～ｕ１６）。また、木の各ノード（節）を用いて、「そのノードを頂点とする部分木のリーフ（葉）に割り当てられた受信機からなる集合」を表す。図３におけるノードｉ２０１は、受信機ｕ５とｕ６からなる集合を表す。

【００７４】

そして、図３に示す２分木の各構成ノードに鍵（ノードキー）が定義される。各受信機には、各受信機が割り当てられているリーフ（葉）から木のルート（頂点）に至るパス上のノードに割り当てられたノードキーが与えられ、受信機はこれらのノードキーを安全なメモリに保持する。木の定義やノードキーの定義、受信機の割り当てやノードキーの配布などは、Ｔｒｕｓｔｅｄ　Ｃｅｎｔｅｒ（ＴＣ）と呼ばれる信頼される管理センタが行なう。

【００７５】

図４に示すように、階層木には１６台の受信機ｕ１～ｕ１６が割り当てられ、ノードは１～３１の３１個、存在する。受信機ｕ４には、ノード１，２，４，９，１９に割り当てられた５個のノードキーが与えられる。すなわち、全受信機数をＮとした場合には、各受信機はｌｏｇＮ＋１個のノードキーを保持することになる。

【００７６】

図５を用いて、このセッティングを用いて秘密情報（たとえば、暗号化されたコンテンツを復号するためのコンテンツキー）をどのようにリボークされない受信機に送信するかについて説明する。ここでは、管理センタ（ＴＣ）が秘密情報の送信者になるとする。いま、受信機ｕ２，ｕ１１，ｕ１２がリボークされる受信機とする。すなわち、受信機ｕ２，ｕ１１，ｕ１２を不正な機器として排除（リボーク）し、それ以外の受信機においてのみ安全に情報を受領、すなわち同報配信される暗号文に基づく復号を行なうことを可能とする。

【００７７】

管理センタ（ＴＣ）が秘密情報の送信を行なう場合、リボーク受信機ｕ２，ｕ１１，ｕ１２が割り当てられているリーフ（葉）から木のルートに至るパス上のノードに割り当てられたノードキーを暗号鍵として使用せず、暗号文のセットを生成して同報送信する。

【００７８】

リボーク受信機ｕ２，ｕ１１，ｕ１２が割り当てられているリーフ（葉）から木のルートに至るパス上のリーフまたはノードに割り当てられたノードキーを使用すると、これらは、リボークすべき受信機が持つキーであるため、リボーク機器において秘密情報を入手できてしまう。従って、これらのキーを用いずに暗号文のセットを生成して同報送信する。

【００７９】

リボーク受信機ｕ２，ｕ１１，ｕ１２が割り当てられているリーフ（葉）から木のルートに至るパス上のノードおよびパスを木から除外すると、１つ以上の部分木が残る。例えば、ノード５を頂点とする部分木、あるいはノード１２を頂点とする部分木などである。

【００８０】

秘密情報の送信者は、それぞれの部分木の頂点に最も近いノード、すなわち、図５に示す例では、ノード５，７，９，１２，１６に割り当てられたノードキーを用いて秘密情報を暗号化した暗号文のセットを送信する。例えば送信秘密情報を暗号化コンテンツの復号に適用するコンテンツキーＫｃであるとし、ノード５，７，９，１２，１６に割り当てられたノードキーをＮＫ５，ＮＫ７，ＮＫ９，ＮＫ１２，ＮＫ１６とすると、秘密情報の送信者は、

Ｅ（ＮＫ５，Ｋｃ），Ｅ（ＮＫ７，Ｋｃ），Ｅ（ＮＫ９，Ｋｃ），Ｅ（ＮＫ１２，Ｋｃ），Ｅ（ＮＫ１６，Ｋｃ）

の暗号文セットを生成して、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。

【００８１】

上記暗号文セットは、リボーク受信機ｕ２，ｕ１１，ｕ１２のみが復号することができず、その他の受信機では復号可能である。このような暗号文セットを生成し送信することで、効率的で安全な秘密情報の伝送が行える。

【００８２】

受信機は、伝送された暗号文のうち、自分が復号できるもの、すなわち、自身が割り当てられたリーフ（葉）からルートに至るまでのパス上のノードに対応するノードキーを用いて暗号化されたものを復号して秘密情報を得ることができる。上記の例では、受信機ｕ４はノード９のノードキーを保持しているので、これを用いて暗号化された暗号文Ｅ（ＮＫ９，Ｋｃ）を復号することができる。このように、リボークされていない受信機が復号できる暗号文は受信した暗号文セット中に必ずひとつ存在する。

【００８３】

［２．Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式］

上記のように、Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式においては、階層木の各ノード（節）を用いて、「そのノードを頂点とする部分木のリーフ（葉）に割り当てられた受信機からなる集合」を表していた。これに対し、Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式においては、階層木の２つのノードｉ，ｊ（ただしｉはｊの先祖であるノード）を用いて、「（ノードｉを頂点とする部分木のリーフ（葉）からなる集合）から（ノードｊを頂点とする部分木のリーフ（葉）からなる集合）を引いた集合」を表す。

【００８４】

たとえば図６のノードｉ２３１，とノードｊ２３２で定義される集合$S_{i,j}$は、受信機ｕ１～ｕ８の集合からｕ５，ｕ６を除いたものであり、すなわち、$S_{i,j}$＝｛ｕ１，ｕ２，ｕ３，ｕ４，ｕ７，ｕ８｝である。ノードｉがノードｊの先祖である（すなわち、ノードｊはノードｉと同一ではなく、ノードｊからルートへのパス上にノードｉが存在する）すべてのノードの組についてこのような集合を定義する。

【００８５】

サブセット$S_{i,j}$に対応する鍵としてサブセットキー$SK_{i,j}$が設定される。サブセットキー$SK_{i,j}$は、ｕ１～ｕ８の集合からｕ５，ｕ６を除いたサブセット$S_{i,j}$＝｛ｕ１，ｕ２，ｕ３，ｕ４，ｕ７，ｕ８｝が共通に保有する鍵として設定され、サブセットキー$SK_{i,j}$を暗号鍵として秘密情報を暗号化した情報を送信することにより、サブセット$S_{i,j}$＝｛ｕ１，ｕ２，ｕ３，ｕ４，ｕ７，ｕ８｝においてのみ復号可能となり、ｕ５，ｕ６をリボーク（排除）することができる。

【００８６】

このようなセッティングでは、ひとつの受信機が所属する集合の個数は、下式によって示される数Ｏ（Ｎ）となる。

【数９】

$$\sum_{k=1}^{\log N}(2^k - k) = O(N)$$

【００８７】
従って、それぞれの集合（サブセット）に鍵（サブセットキー）を独立に割り当てたのでは、各受信機がＯ（Ｎ）個のサブセットキーを安全に保持する必要がある。しかし、これは、総受信機数Ｎの増大に伴い飛躍的に増大し、これらの大量の情報を各機器に安全に保管させることは現実的に困難である。
【００８８】
このため、Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式では以下に述べる工夫を用いている。前述したＣｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式と同様に、管理センタ（ＴＣ）が階層木の定義やサブセットの定義、鍵の定義、配布などを行うものとする。
【００８９】
まず、図７（Ａ）に示すように、管理センタ（ＴＣ）は、ある内部ノード（すなわち、リーフ（葉）でないノード）ｉに注目し、そのノードｉのラベルをＬＡＢＥＬｉとしてＣビットの値Ｓをランダムに選択する。
【００９０】
次に、図７（Ｂ）の図に示すように、ＬＡＢＥＬｉ＝Ｓを、Ｃビット入力、３Ｃビット出力の擬似乱数生成器Ｇに入力する。この出力を左から（最上位ビット側から）Ｃビットずつに区切り、それぞれ$G_L$（Ｓ），$G_M$（Ｓ），$G_R$（Ｓ）とする。そして、$G_L$（Ｓ）を、図７（Ａ）に示すノードｉの左側の子ノードｋのラベルとし、また$G_R$（Ｓ）をノードｉの右側の子ノードのラベルとする。
【００９１】
いま、この処理により、図７においてノードｉの左側の子であるノードｋについて、ノードｉを始点にした場合のノードｋのラベル$LABEL_{i,k}$は、$LABEL_{i,k}=G_L$（Ｓ）となった。これをＴとおく。次に、今度はノードｋのラベル$LABEL_{i,k}=G_L$（Ｓ）＝Ｔを、図７（Ｂ）に示す擬似乱数生成器Ｇに入力し、その出力を左からＣビットずつに区切った、$G_L$（Ｔ），$G_M$（Ｔ），$G_R$（Ｔ）を、それぞれ以下のように設定する。
$G_L$（Ｔ）＝ノードｉを始点にした場合のノードｋの左側の子ノードＬＣ（ｋ）のラベル$LABEL_{i,LC(k)}$
$G_M$（Ｔ）＝ノードｉを始点にした場合のノードｋの鍵（これを集合$S_{i,k}$に対応するサブセットキー$SK_{i,k}$とする）
$G_R$（Ｔ）＝ノードｉを始点にした場合のノードｉの右側の子ノードＲＣ（ｋ）のラベル$LABEL_{i,RC(k)}$
【００９２】
この処理を繰り返すことにより、ノードｉを始点とした場合の、その子孫となるすべてのノードに対応するラベルを作り出す。なお、上記の定義によれば集合$S_{i,i}$は空集合であり、ノードｉを始点とした場合に、ノードｉの鍵というものは不要であるため、$LABEL_i$を擬似乱数生成器Ｇに入力した出力の中央部分である$G_M$（Ｓ）は使われないことに注意されたい。
【００９３】

図７（Ａ）の例で示すと、始点であるノードｉのラベルＳが定められ、$G_R$（Ｓ）がノードｉを始点とした場合のｉの右の子ノードのラベルとなり、さらにそれを擬似乱数生成器Ｇに入力して得られた$G_L$（$G_R$（Ｓ））が、ノードｉを始点とした場合のノードｊのラベル$LABEL_{i,j}$となる。ノードｉを始点とした場合の、その子孫となるすべてのノードに対応するラベルを作り出す処理を、すべての内部ノードｉに対して行う。

【００９４】

これらの処理はシステムのセットアップ時に、管理センタ（ＴＣ）によって行われるが、擬似乱数生成器（あるいは擬似乱数生成関数）Ｇは、管理センタ（ＴＣ）によって定められ公開されており、これを用いることによって、$LABEL_{i,j}$を与えられた受信機は、ノードｉを始点とした場合の、ノードｊの子孫となるすべてのノードｎのラベル$LABEL_{i,n}$を計算することおよび、ノードｉを始点とした場合の、ノードｊおよびその子孫ノードｎのサブセットキー$SK_{i,n}$を計算することが可能となる。

【００９５】

このような設定により、図８（Ａ）に示すように、ある受信機ｕは、それが割り当てられたリーフ（葉）から木の頂点へのパス上のそれぞれの内部ノードｉについて、ノードｉを始点として、このリーフ（葉）ｕからｉへのパスから直接枝分かれしているノードであるノードａ，ｂ，ｃのラベルのみを保持しておけばよいことになる。

【００９６】

これらのノードａ，ｂ，ｃおよびその子孫となるノードの、ノードｉを始点としたサブセットキーを作り出すことが可能となる。図８（Ａ）では、ノードｉに注目したときに、ｕからｉへのパスから直接枝分かれしているノードはａ，ｂ，ｃの３つであり、受信機ｕはこれら３つのラベルをシステムのセットアップ時に、管理センタ（ＴＣ）から与えられて保持する。

【００９７】

リーフｕは、ノードａのラベル$LABEL_{i,a}$に基づく擬似乱数生成器Ｇの処理によって、サブセット$S_{i,a}$に対応するサブセットキー$SK_{i,a}$を求めることができる。すなわち、

$G_M$（$LABEL_{i,a}$）＝$SK_{i,a}$となる。

サブセット$S_{i,a}$は、図８（ａ）に示すように、ノードａを頂点とした部分木のリーフをリボーク機器として設定したサブセットであり、ノードｉを頂点とした部分木のリーフのうちノードａを頂点とした部分木のリーフ以外のリーフのみを情報配信対象として設定されるサブセットである。

【００９８】

また、リーフｕは、ノードｂのラベル$LABEL_{i,b}$に基づく擬似乱数生成器Ｇの処理によって、サブセット$S_{i,b}$に対応するサブセットキー$SK_{i,b}$を求めることができる。すなわち、

$G_M$（$LABEL_{i,b}$）＝$SK_{i,b}$となる。

サブセット$S_{i,b}$は、図８（ｂ）に示すように、ノードｂを頂点とした部分木のリーフをリボーク機器として設定したサブセットであり、ノードｉを頂点とした部分木のリーフのうちノードｂを頂点とした部分木のリーフ以外のリーフのみを情報配信対象として設定されるサブセットである。

【００９９】

また、リーフｕは、ノードｃのラベル$LABEL_{i,c}$に基づく擬似乱数生成器Ｇの処理によって、サブセット$S_{i,c}$に対応するサブセットキー$SK_{i,c}$を求めることができる。すなわち、

$G_M$（$LABEL_{i,c}$）＝$SK_{i,c}$となる。

サブセット$S_{i,c}$は、図８（ｃ）に示すように、ノードｃ（リーフｃ）をリボーク機器として設定したサブセットであり、ノードｉを頂点とした部分木のリーフのうちリーフｃ以外のリーフのみを情報配信対象として設定されるサブセットである。

【０１００】

ｉを始点とする階層木において、リーフｕ以外のリーフをリボークする構成は、これら３つ以外にも様々設定可能である。例えば図８（ａ）のリーフｄ２５１のみをリボーク対象とする場合は、サブセット$S_{i,d}$を設定し、サブセットキー$SK_{i,d}$を適用することが必要である。しかし、各ノード、リーフに対応する鍵、すなわちサブセットキーは、上位のラベルに基づく擬似乱数生成処理により生成可能である。従って、リーフｕは、リーフｄ２５１のリボークに対応するサブセットキー$SK_{i,d}$を、リーフｕが保有するノードａのラベル$LABEL_{i,a}$に基づいて生成可能となる。

【０１０１】

その他のサブセット構成についても同様であり、図８（Ａ）に示すように、ある受信機ｕは、それが割り当てられたリーフ（葉）から木の頂点へのパス上のそれぞれの内部ノードｉについて、ノードｉを始点として、このリーフ（葉）ｕからｉへのパスから直接枝分かれしているノードであるノードａ，ｂ，ｃのラベルのみを保持しておけばよいことになる。

【０１０２】

図９は全受信機数Ｎ＝１６の設定の場合に各受信機が保持すべきラベルを示す図である。いま、受信機ｕ４を考えると、それが割り当てられたリーフ（葉）であるノード１９から頂点１へのパス上の内部ノード１，２，４，９が始点（ノードｉ）となる。ノード１を始点とすると、ノード１９からノード１へのパスから直接枝分かれしているノードは３，５，８，１８の４つであるため、受信機ｕ４は４つのラベル、すなわち、

$LABEL_{1,3}$，
$LABEL_{1,5}$，
$LABEL_{1,8}$，
$LABEL_{1,18}$，
を保持する。

【０１０３】

同様に、ノード２を始点とした場合には、

$LABEL_{2,5}$，
$LABEL_{2,8}$，
$LABEL_{2,18}$，
の３つのラベルを保持する。

【０１０４】

ノード４を始点とした場合には、

$LABEL_{4,8}$，
$LABEL_{4,18}$，
の２つのラベルを保持する。

【０１０５】

ノード９を始点とした場合には、

$LABEL_{9,18}$，
の１つのラベルを保持する。

【０１０６】

また、リボークすべき受信機がないという特別な場合に使用する全受信機を含む集合（これをサブセット$S_{1,\phi}$と表すことにする）に対応するラベル

$LABEL_{1,\phi}$，
を１つ保持する。

【０１０７】

すなわち、図９の構成においてｕ４が持つＬＡＢＥＬをまとめると、図９にも記載しているように、

ｉ＝１に対してｊ＝３，５，８，１８の４つのラベル
ｉ＝２に対してｊ＝５，８，１８の３つのラベル
ｉ＝４に対してｊ＝８，１８の２つのラベル

ｉ＝９に対してｊ＝１８の１つのラベル
リボークなしの場合用のＬＡＢＥＬを１つ
の計１１個のラベルとなる。

【０１０８】

ただし、ここでは説明を統一するため、サブセット$Ｓ_{1,\phi}$に対応するラベルとしているが、ラベルではなくサブセット$Ｓ_{1,\phi}$に対応するに対応するサブセットキーを直接保持してもよい。

【０１０９】

上記のように、各受信機は、リーフ（葉）からルートへのパス上の各内部ノードについて、その内部ノードの高さ分だけのラベルと特別な１つのラベルを保持する必要があるから、送受信機数をＮとした場合に各受信機が保持するラベル数は、下記式によって算出される数となる。

【数１０】

$$1+\sum_{k=1}^{\log N} k = \frac{1}{2}\log^2 N + \frac{1}{2}\log N + 1$$

【０１１０】

各受信機は、上記式によって示される数のラベルを保持し、公開されている擬似乱数生成関数Ｇを用いることにより必要とするサブセットキーを作り出すことができる。受信機はこれらのラベルを安全に保持する必要がある。

【０１１１】

［３．一方向性置換木を用いたＳＤ方式のラベル数削減構成］

次に、本発明に係る一方向性置換木を用いたＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式のラベル数の削減構成について説明する。上述したＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式を観察すると、以下のことがわかる。

【０１１２】

すなわち、ラベル$ＬＡＢＥＬ_{i,j}$は、
（Ａ）受信機に直接、管理センタ（ＴＣ）から与えられる場合と、
（Ｂ）受信機がそれ以外のラベルから擬似乱数生成器Ｇを用いて導出する場合と、
があるが、
ノードｉとノードｊが親子の関係（距離１、すなわち連続する階層にある）であるラベルについては、上記の（Ｂ）の場合は存在せず、すべて、（Ａ）受信機に直接、管理センタ（ＴＣ）から与えられる場合しかありえない。

【０１１３】

これは、ある受信機が$ＬＡＢＥＬ_{i,j}$を擬似乱数生成器Ｇを用いて作り出すためには、ノードｊの先祖となるノードｋを用いた$ＬＡＢＥＬ_{i,k}$を知る必要があるが、ノードｉ，ｊが親子関係であるため、ノードｊの先祖であり、ノードｉの子孫となるようなノードｋは存在せず、また、$ＬＡＢＥＬ_{i}$はどの受信機にも与えられていないためである。

【０１１４】

図１０の構成例を参照して説明する。$ＬＡＢＥＬ_{2,8}$は、受信機ｕ４には直接、管理センタ（ＴＣ）から与えられるが、受信機ｕ５には直接は与えられず、受信機ｕ５は、管理センタ（ＴＣ）から与えられた$ＬＡＢＥＬ_{2,4}$から擬似乱数生成器Ｇを用いて$Ｇ_{L}$（

ＬＡＢＥＬ$_{2,4}$）を計算することによりＬＡＢＥＬ$_{2,8}$を導出する。

【０１１５】

これに対し、図１１に示すように、ノード２とノード５が親子関係になるＬＡＢＥＬ$_{2,5}$は、サブセットＳ$_{2,5}$に属している受信機ｕ１，ｕ２，ｕ３，ｕ４には直接与えられ、これ以外の受信機はその集合に属していないため、計算で導出することもできない。すなわち、このようなラベルは受信機に対し直接、管理センタ（ＴＳ）から与えられるだけで、擬似乱数生成器Ｇを用いて導出されることはない。

【０１１６】

また、ＳＤ方式において、あるノードｉが異なる２つのノードｊ，ｋの親ノードであり、ノードｊがそれらとは別のノードｎの親ノードであるとき、サブセットＳ$_{j,n}$に属する受信機は必ずサブセットＳ$_{i,k}$にも所属することがわかる。

【０１１７】

たとえば図１２に示すように、サブセットＳ$_{9,18}$に属している受信機Ｕ４は、サブセットＳ$_{4,8}$、サブセットＳ$_{2,5}$、サブセットＳ$_{1,3}$のいずれにも属している。すなわち、

Ｓ$_{9,18}$＝｛ｕ４｝

Ｓ$_{4,8}$＝｛ｕ３，ｕ４｝

Ｓ$_{2,5}$＝｛ｕ１，ｕ２，ｕ３，ｕ４｝

Ｓ$_{1,3}$＝｛ｕ１，ｕ２，ｕ３，ｕ４，ｕ５，ｕ６，ｕ７，ｕ８｝

である。

【０１１８】

またサブセットＳ$_{4,8}$に属する受信機ｕ４以外の受信機である受信機ｕ３も、サブセットＳ$_{2,5}$、サブセットＳ$_{1,3}$のいずれにも属している。

【０１１９】

本発明では、ノードｉとノードｊが親子関係になるラベルＬＡＢＥＬ$_{i,j}$と、リボークすべき受信機がないという特別な場合に使用する全受信機を含む集合であるサブセットＳ$_{1,\phi}$に対応するラベルであるＬＡＢＥＬ$_{1,\phi}$に対して、落とし戸つき一方向性置換を適用した鍵の木構造、すなわち一方向性置換木を適用することにより受信機が保持するラベル数を削減する。

【０１２０】

上述したＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式においては各受信機は、ノードｉとノードｊが親子関係になるラベルＬＡＢＥＬ$_{i,j}$を、受信機が割り当てられたリーフ（葉）から木の頂点へのパス上の内部ノード１つにつき１つずつ、合計ｌｏｇＮ個保持している。本発明では、一方向性置換木を適用することにより、これらのラベルと、リボークすべき受信機がないという特別な場合に使用する全受信機を含む集合であるサブセットＳ$_{1,\phi}$に対応するラベルであるＬＡＢＥＬ$_{1,\phi}$の合計ｌｏｇＮ＋１個のラベルを１つの値から導出可能な設定とすることで、受信機の保持すべきラベル数を削減する。

【０１２１】

オリジナルのＳＤ方式では、図９を参照して説明したように、受信機ｕ４は計１１個のラベル、すなわち、

ｉ＝１に対してｊ＝３，５，８，１８の４つのラベル

ＬＡＢＥＬ$_{1,3}$，

ＬＡＢＥＬ$_{1,5}$，

ＬＡＢＥＬ$_{1,8}$，

ＬＡＢＥＬ$_{1,18}$，

ｉ＝２に対してｊ＝５，８，１８の３つのラベル

ＬＡＢＥＬ$_{2,5}$，

ＬＡＢＥＬ$_{2,8}$，

ＬＡＢＥＬ$_{2,18}$，

ｉ＝４に対してｊ＝８，１８の２つのラベル

ＬＡＢＥＬ$_{4,8}$，
ＬＡＢＥＬ$_{4,18}$，
ｉ＝９に対してｊ＝１８の１つのラベル
ＬＡＢＥＬ$_{9,18}$，
リボークなしの場合用のＬＡＢＥＬを１つ
ＬＡＢＥＬ$_{1,\phi}$，
計１１のラベルを安全に保持する必要があったが、本発明の構成を適用することにより、ノードｉ，ｊが親子関係になるラベル、すなわち、
ＬＡＢＥＬ$_{1,3}$，
ＬＡＢＥＬ$_{2,5}$，
ＬＡＢＥＬ$_{4,8}$，
ＬＡＢＥＬ$_{9,18}$，
さらに、リボークなしの場合用のＬＡＢＥＬである
ＬＡＢＥＬ$_{1,\phi}$，
これらのラベルを、受信機は保持することが必要であるが、本発明では、一方向性置換木を適用することにより、これらのラベルと、リボークすべき受信機がないという特別な場合に使用する全受信機を含む集合であるサブセットＳ$_{1,\phi}$に対応するラベルであるＬＡＢＥＬ$_{1,\phi}$の合計ｌｏｇＮ＋１個のラベルを１つの値から導出可能な設定とすることで、受信機の保持すべきラベル数を削減する。

【０１２２】

なお、本発明において適用する落とし戸つき一方向性置換とは、ｘからｙを計算するのは簡単であるが、その逆の計算、すなわちｙからｘを計算する処理は、ある秘密情報（落とし戸）を知っているものだけが実行でき、この秘密情報（落とし戸）を知らないものにとっては困難（ほぼ不可能）である置換処理ｙ＝Ｆ（ｘ）である。

【０１２３】

［４．一方向性置換木の構成例］

以下、本発明にかかる一方向性置換木を用いた階層木構成に基づく情報配信構成について説明する。なお、本明細書の説明において用いている「一方向性置換木」とは、一般的な用語ではなく本発明の説明のために用いる言葉であり、ある特性を持つ木構造を定義した言葉である。

【０１２４】

「一方向性置換木」の定義について説明する。

Ｎ個の葉を持つ完全２分木が一方向性置換木であるとは、図１３に示すように、最上位のノードであるルートを１、それ以降のノードを上位の左から順に２，３，...，２Ｎ－１と幅優先（breadth first order）で各ノードにノード番号を設定した場合に、ノードｉに対応する値、すなわちノード対応値として値ｘ$_i$（ｉ＝１，２，...，２Ｎ－１）を設定し、ｉ＝１，２，...，Ｎ－１について、下記式

【数１１】

$$x_i = F^{-1}(x_{\lfloor i/2 \rfloor} + i)$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

・・・（数式１）

が成り立つ木構造を一方向性置換木というものとする。上記式において、

$F^{-1}$は、落とし戸つき一方向性置換Ｆの逆置換である。

なお、落とし戸つき一方向性置換の例として、ＲＳＡ暗号が挙げられる。ＲＳＡ暗号はパラメータとして法Ｍ、公開指数ｅ、秘密指数ｄを用い、

（公開）置換$F = x^{e} \bmod M$

（秘密）逆置換$F^{-1} = x^{d} \bmod M$

を用いる暗号方式である。ＲＳＡ暗号の解説は、たとえばＡ．Ｊ．Ｍｅｎｅｚｅｓ，Ｐ．Ｃ．ｖａｎ Ｏｏｒｓｃｈｏｔ ａｎｄ Ｓ．Ａ．Ｖａｎｓｔｏｎｅ著，"Ｈａｎｄｂｏｏｋ ｏｆ Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ，"ＣＲＣ Ｐｒｅｓｓ，１９９６に紹介されている．

【０１２５】

また、別の例として、上記式（数式１）の代わりに、ハッシュ関数等の一方向性関数ｈを適用した例として、下記式

【数１２】

$$x_i = F^{-1}(x_{\lfloor i/2 \rfloor} + h(i))$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

・・・（数式２）

が成り立つ木構造を一方向性置換木としてもよい。

関数ｈは、任意長の入力に対し一定の長さの出力を出す関数であり、ｘからｙを計算するのは簡単だが、その逆計算は、困難であるような関数ｙ＝Ｈ（ｘ）である。このような関数は一方向性関数またはハッシュ関数と呼ばれ、例えばＭＤ４、ＭＤ５や，１６０ビットの出力を出すＳＨＡ－１などが有名である。これらの関数も上述の"Ｈａｎｄｂｏｏｋ ｏｆ Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ"に紹介されている。

【０１２６】

一方向性置換木を構成する各ノードｉに対応して設定されるノード対応値$x_i$と、各ノード対応値の算出に適用する置換Ｆに対応する演算（ｆ）と、逆置換$F^{-1}$に対応する演算（$f^{-1}$）との設定関係を図で表すと、図１３のようになる。

【０１２７】

図に示すように、あるノードの値からその親ノードの値を計算することは、落とし戸つき一方向置換の順方向置換Ｆを用いた計算ｆによって行え、逆にあるノードの値からその子ノードの値を計算することは逆置換$F^{-1}$を用いた計算$f^{-1}$によって行える。ここで、逆置換を計算することは落とし戸（秘密）を知っているものだけが現実的に行え、それを知らないものには困難であることに注意されたい。

【０１２８】

落とし戸つき一方向性置換のひとつであるＲＳＡ暗号を用いて、葉がＮ個である２分木の一方向性置換木を構成するアルゴリズムについて、図１４を参照して説明する。

【０１２９】

まず、ステップＳ１０１において、数$x_1 \in Z^{*}_{M}$をランダムに選択する。なお、$x_1 \in Z^{*}_{M}$は、$x_1$が、巡回群$Z^{*}_{M}$の生成元であることを意味する。

【０１３０】
次にステップＳ１０２～Ｓ１０５において、ｉをカウンタとして、ｉ＝２～２Ｎ－１まで、ｉを１つずつ増加させながら、下記式（数式３）に従ってノード対応値$x_i$を算出する。
【数１３】

$$x_i = (x_{\lfloor i/2 \rfloor} + i)^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

・・・（数式３）
【０１３１】
上記式（数式３）は、図１３における逆置換に相当する演算$f^{-1}$を上位ノードから順に算出している処理に相当する。
【０１３２】
ステップＳ１０２～Ｓ１０５において、ｉをカウンタとして、ｉ＝２～２Ｎ－１まで、ｉを１つずつ増加させながら、上記式（数式３）に従ってノード対応値$x_i$が算出されると、ステップＳ１０６において、２Ｎ－１個の｜Ｍ｜ビットの数$x_1$，$x_2$，...，$x_{2^N-1}$を出力して終了する。値$x_i$が一方向置換木のノードｉに対応する値、すなわちノード対応値となる。ここで、葉の数がＮである完全２分木のノードの総数は２Ｎ－１である点に注意されたい。
【０１３３】
なお、図１４に示す処理フローにおけるステップ１０において適用したノード対応値の算出のための演算は、ハッシュ関数ｈを適用し、下記式（数式４）を適用して実行する構成としてもよい。
【数１４】

$$x_i = (x_{\lfloor i/2 \rfloor} + h(i))^d \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

・・・（数式４）
【０１３４】
［５．一方向性置換木を適用した情報配信処理例］
次に、上述した一方向性置換木を適用した情報配信処理例について説明する。以下、
（５－１）セットアップ処理
（５－２）情報配信処理

（５－３）受信および復号処理

の各処理について順次、説明する。

【０１３５】

（５－１）セットアップ処理

セットアップ処理はシステムの立ち上げ時に１度だけ行う。これ以降の情報配信および受信と復号の処理は、送信すべき情報が生じる毎に実行する。たとえば新しいコンテンツを格納したＤＶＤディスクなどのコンテンツ格納記録媒体が作成され、ユーザに対して配布される毎、あるいはインターネットを介して暗号化コンテンツが配信される毎に繰り返し行う。

【０１３６】

セットアップ処理は、以下のステップ１～４の処理によって実行する。各ステップについて説明する。

【０１３７】

ａ．ステップ１

まず、管理センタ（ＴＣ）は、２分木でありＮ個のリーフ（葉）を持つ階層木を定義する。なお、この階層木は、上述の一方向性置換木とは別である。階層木中の各ノードに対応する識別子として、ｋ（ｋ＝１，２，・・・，２Ｎ－１）を設定する。ただしルートを１とし、以下、下層ノードについて順次、幅優先（ｂｒｅａｄｔｈ　ｆｉｒｓｔ　ｏｒｄｅｒ）で、識別子（番号）付与を行う。すなわち、図１５に示すようなノード番号（ｙ）の設定を行なう。この処理により２分木中の各ノードにｙ＝１～２Ｎ－１のノード番号が設定される。

【０１３８】

受信機ｕｍ（ｍ＝１，２，...，Ｎ）を木の各葉（リーフ）に割り当てる。図１５の例では、ノード番号ｙ＝１６～３１に受信機ｕ１～ｕ１６の１６台の受信機が割り当てられる。

【０１３９】

次に、各内部ノードｉ（ｉ＝１，２，・・・，Ｎ－１）について、ノードｉの子孫であるノードｊに対応するサブセット$S_{i,j}$を定義する。さらに、上で定義されたすべてのサブセット$S_{i,j}$の中で、ノードｉとノードｊが親子関係になっているものを第１の特別なサブセット（スペシャルサブセット：Ｓｐｅｃｉａｌ　Ｓｕｂｓｅｔ）$SS_{i,j}$と表すことにする。ここで、木のルートを除く各ノードは、それぞれ唯一の親ノードを持つので、$SS_{i,j}$のｊには、ｊ＝２，３，・・・，２Ｎ－１なるｊがただ１度ずつ使用されることに注意されたい。さらに、リボークする受信機がひとつもない場合に使用する、全受信機を含む第２の特別なサブセット$SS'_{1,\phi}$を定義する。

【０１４０】

ｂ．ステップ２

管理センタ（ＴＣ）は、ＲＳＡ暗号のパラメータである法Ｍ、公開指数ｅ、秘密指数ｄを生成し、法Ｍと公開指数ｅを公開する。ここで、法Ｍのサイズを｜Ｍ｜ビットとする。例えば、｜Ｍ｜ビット＝１０２４ビットである。さらに、擬似乱数生成器ＧおよびＣビット（例えば１２８ビット）出力のハッシュ関数Ｈを選択して公開する。擬似乱数生成器Ｇは、先に図７を参照して説明した擬似乱数生成器Ｇであり、Ｃビット入力に対して３Ｃビットの擬似乱数を出力するものであり、前述のＳＤ方式において適用されているＮｏａｒらの論文において説明されている擬似乱数生成器と同様のものである。

【０１４１】

次に、

葉（リーフ）の数＝Ｎ、

ＲＳＡ暗号のパラメータである法Ｍ、秘密指数ｄ

を入力して、先に図１４のフローを参照して説明したアルゴリズムに従って葉がＮ個である２分木の一方向性置換木を生成し、各ノードｉの対応値$x_i$を算出する。なお、ここで、各ノードｉの対応値$x_i$の算出においては、前述の式（数式３）または式（数式４）

のいずれかを適用する。

【０１４２】

管理センタ（ＴＣ）は、上述の処理において定めた値$x_1$を、リボークする受信機がひとつもない場合に使用する全受信機を含む第２の特別なサブセット$SS'_{1,\phi}$のラベル$LABEL_{1,\phi}$の生成元データとしての中間ラベル（Ｉｎｔｅｒｍｅｄｉａｔｅ Ｌａｂｅｌ，ＩＬ）として設定する。すなわち、

$IL_{1,\phi}=x_1$

とする。

【０１４３】

第２の特別なサブセット$SS'_{1,\phi}$のラベルを$LABEL_{1,\phi}$とし、$LABEL_{1,\phi}$は、上記の中間ラベル$IL_{1,\phi}$に対するハッシュ（Ｈ）によって算出する値とする。すなわち、

$LABEL_{1,\phi}=H(IL_{1,\phi})$

である。

【０１４４】

さらに、すべてのサブセット$S_{i,j}$の中で、ノードｉとノードｊが親子関係になっている第１の特別なサブセット$SS_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応するラベルの生成元データとしての中間ラベル$IL_{i,j}$を下記のように定める。すなわち、前述の処理（図１４参照）によってノード１から２Ｎ－１に対応する値として設定した$x_1$から$x_{2N-1}$の中のルート対応値$x_1$を除く$x_y$（ｙ＝２，３，・・・，２Ｎ－１）をノードｙの兄弟ノードと親ノードで指定される第１の特別なサブセット$SS_{P(y),S(y)}$に対応する中間ラベル$IL_{P(y),S(y)}$とする。すなわち、

$x_y=IL_{P(y),S(y)}$

とする。

なお、Ｐ（ｉ）はノードｉの親ノードであり、Ｓ（ｉ）はノードｉの兄弟ノードである。

【０１４５】

図１６に具体的な例を示す。図１６において、ノードｙ３０１にはノード対応値としての$x_y$が割り当てられる。なお、$x_y$を含むすべてのノード対応値は前述の式（式１）を満足する値であり、

$x_y=IL_{P(y),S(y)}$

である。

【０１４６】

ノードｙ３０１の親ノードは、Ｐ（ｙ）３０２であり、兄弟ノードはＳ（ｙ）３０３である。ノードｙ３０１の兄弟ノードＳ（ｙ）３０３と親ノードＰ（ｙ）３０２で指定される第１の特別なサブセット$SS_{P(y),S(y)}$は、図１６に示すサブセット$SS_{P(y),S(y)}$３１０である。

【０１４７】

このとき、サブセット$SS_{P(y),S(y)}$３１０に対応するラベルは、$LABEL_{P(y),S(y)}$となるが、

$LABEL_{P(y),S(y)}$を、中間ラベル$IL_{P(y),S(y)}$（これはノードｙ３０１のノード対応値$x_y$に等しい）に基づくハッシュ値として設定する。すなわち、

$LABEL_{P(y),S(y)}=H(IL_{P(y),S(y)})$

である。

上記式は、

$LABEL_{P(y),S(y)}=H(x_y)$

と等価である。

【０１４８】

一般式として示すと、すべてのサブセット$S_{i,j}$の中で、ノードｉとノードｊが親子

関係になっている第１の特別なサブセットＳＳ$_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応するラベルＬＡＢＥＬ$_{i,j}$は、中間ラベルＩＬ$_{i,j}$に基づくハッシュ値、すなわち、

ＬＡＢＥＬ$_{i,j}$＝Ｈ（ＩＬ$_{i,j}$）

として算出する。

【０１４９】

なお、前述したように、リボークする受信機がひとつもない場合に使用する全受信機を含む第２の特別なサブセットＳＳ'$_{1,\phi}$のラベルＬＡＢＥＬ$_{1,\phi}$についても中間ラベルＩＬ$_{1,\phi}$に対するハッシュ（Ｈ）によって算出可能、すなわち、

ＬＡＢＥＬ$_{1,\phi}$＝Ｈ（ＩＬ$_{1,\phi}$）

である。

【０１５０】

なお、本例では、中間ラベルに基づくラベルの算出処理にハッシュを適用した例を説明しているが、ハッシュ以外の演算処理によって算出する構成としてもよい。ただし、一方向性関数であることが望ましい。

【０１５１】

管理センタは、ステップ２において、

（ａ）リボークする受信機がひとつもない場合に使用する全受信機を含む全体木に対応する第２の特別なサブセットＳＳ'$_{1,\phi}$のラベルＬＡＢＥＬ$_{1,\phi}$と、

（ｂ）ノードｉとノードｊが親子関係になっている第１の特別なサブセットＳＳ$_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応するラベルＬＡＢＥＬ$_{i,j}$と、

上記（ａ），（ｂ）の特別なサブセット対応のラベルを、それぞれ

中間ラベルＩＬ$_{i,\phi}$のハッシュ値、

中間ラベルＩＬ$_{i,j}$のハッシュ値

として設定する処理を実行する。

【０１５２】

なお、中間ラベルの値は、ノード対応値ｘ$_i$の値であり、先に図１４を参照して説明したアルゴリズムに従って算出された値であり、前述の式（数式３または数式４）を満足する値である。すなわち、

ＩＬ$_{1,\phi}$＝ｘ$_1$

また、ｙ＝１，２，・・・，Ｎ－１に対して、

ＩＬ$_{y,2y}$＝ｘ$_{2y+1}$

ＩＬ$_{y,2y+1}$＝ｘ$_{2y}$

となる。

【０１５３】

図１７に、（ａ）リボークする受信機がひとつもない場合に使用する全受信機を含む全体木に対応する第２の特別なサブセットＳＳ'$_{1,\phi}$のラベルＬＡＢＥＬ$_{1,\phi}$と、（ｂ）ノードｉとノードｊが親子関係になっている第１の特別なサブセットＳＳ$_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応するラベルＬＡＢＥＬ$_{i,j}$との生成元データである中間ラベル（ＩＬ）としてのノード対応値ｘ$_i$の設定処理例を示す。

【０１５４】

図１７において［ｉ　ｘ$_k$　ｊ］は、

ｘ$_k$＝ＩＬ$_{i,j}$

を示す。ただしｉはｊの先祖である。

例えば［１　ｘ$_3$　２］は、

ｘ$_3$＝ＩＬ$_{1,2}$

であることを示している。

【０１５５】

このように、ノード対応値$x_i$は、上述の第１の特別なサブセット$SS_{i,}$と、第２の特別なサブセット$SS'_{1,\phi}$のラベルを算出可能な中間ラベルに対応する値として設定される。

【０１５６】

管理センタ（ＴＣ）は、設定した中間ラベルに基づいて、ハッシュ値を算出し、（ａ）リボークする受信機がひとつもない場合に使用する全受信機を含む第２の特別なサブセット$SS'_{1,\phi}$のラベル$LABEL_{1,\phi}$と、（ｂ）ノードｉとノードｊが親子関係になっている第１の特別なサブセット$SS_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応するラベル$LABEL_{i,j}$を決定する。

【０１５７】

図１８に、先に説明した図１６に対応する具体例を示す。ノードｙ３０１を図に示すように、ノード番号８であるとする。ノードｙ３０１にはノード対応値としての$x_8$が割り当てられる。ノードｙ３０１の親ノードは、Ｐ（ｙ）３０２でありノード番号４、兄弟ノードＳ（ｙ）３０３のノード番号は９である。ノードｙ３０１の兄弟ノードＳ（ｙ）３０３と親ノードＰ（ｙ）３０２で指定される第１の特別なサブセット$SS_{P(y),S(y)}$は、図１６に示すサブセット$SS_{4,9}$３１０である。このとき、$SS_{4,9}$３１０に対応するラベルの生成元データとしての中間ラベルは、

$x_8 = IL_{P(y),S(y)}$

$= IL_{4,9}$

である。

【０１５８】

サブセット$SS_{4,9}$３１０に対応するラベルは、$LABEL_{4,9}$であり、$LABEL_{4,9}$を、中間ラベル$IL_{4,9}$（これはノードｙ３０１のノード対応値$x_8$に等しい）に基づくハッシュ値として設定する。すなわち、

$LABEL_{4,9} = H(IL_{4,9})$

である。

上記式は、

$LABEL_{4,9} = H(x_8)$

と等価である。

【０１５９】

管理センタは、上述したように、ステップ２において、

（ａ）リボークする受信機がひとつもない場合に使用する全受信機を含む全体木に対応する第２の特別なサブセット$SS'_{1,\phi}$のラベル$LABEL_{1,\phi}$と、

（ｂ）ノードｉとノードｊが親子関係になっている第１の特別なサブセット$SS_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応するラベル$LABEL_{i,j}$と、

を決定する。各ラベルは、ノード対応値に等しい中間ラベルのハッシュ値によって算出する。

【０１６０】

ｃ．ステップ３

次に、管理センタ（ＴＣ）は、ノードｉとノードｊが親子関係になっている第１の特別なサブセット$SS_{i,j}$のラベル$LABEL_{i,j}$を擬似乱数生成器Ｇに入力し、ノードｉを始点とした、ノードｊの子ノードのラベル$LABEL_{i,LC(j)}$と、$LABEL_{i,RC(j)}$を求める。

【０１６１】

すなわち、ビット数Ｃの$LABEL_{i,j}$を擬似乱数生成器Ｇに入力して得られる３Ｃビットの擬似乱数の上位Ｃビットである$G_L(LABEL_{i,j})$を、ノードｉを始点とした、ノードｊの左の子ノードＬＣ（ｊ）に対応する（特別でない）サブセット$S_{i,LC(j)}$のラベル$LABEL_{i,LC(j)}$として設定し、さらに、ビット数Ｃの$LABEL_{i,j}$を擬似乱数生成器Ｇに入力して得られる３Ｃビットの擬似乱数の下位Ｃビット

であるG$_R$（ＬＡＢＥＬ$_{i,j}$）を、ノードｉを始点とした、ノードｊの右の子ノードＲＣ（ｊ）に対応する（特別でない）サブセットＳ$_{i,RC(j)}$のラベルＬＡＢＥＬ$_{i,RC(j)}$として設定する。すなわち、

ＬＡＢＥＬ$_{i,LC(j)}$＝G$_L$（ＬＡＢＥＬ$_{i,j}$）

ＬＡＢＥＬ$_{i,RC(j)}$＝G$_R$（ＬＡＢＥＬ$_{i,j}$）

として、各ラベルを設定する。

【０１６２】

さらにこれらの出力（ラベル）を擬似乱数生成器Ｇに繰り返し入力することで、ノードｉを始点とした、ノードｊの子孫であるすべてのノードに対応するラベルを求める。これをすべての特別なサブセットＳＳ$_{i,j}$のラベルに対して行い、ステップ１で定義したすべてのサブセットＳ$_{i,j}$のラベルを求める。

【０１６３】

ｄ．ステップ４

次に管理センタ（ＴＣ）は、受信機ｕｍに対して提供するラベル、すなわち、受信機ｕｍが保管すべきラベルを決定する。

【０１６４】

まず、オリジナルのＳＤ方式において受信機ｕｍに対して与えるラベルを仮選択ラベルとして選択する。これは、受信機ｕｍが割り当てられたリーフ（葉）からルートに至るパスｍ（ｐａｔｈ－ｍ）上の内部ノードｉを始点とし、このリーフ（葉）からｉまでのパスから直接枝分かれしたノードｊに対応するサブセットＳ$_{i,j}$のラベルＬＡＢＥＬ$_{i,j}$と、上記の第２の特別なサブセットＳＳ'$_{1,\phi}$に対応するラベルＬＡＢＥＬ$_{1,\phi}$である。

【０１６５】

図１９以下を参照して受信機に提供するラベルの決定処理について説明する。例えば、図１９のノード番号１９に対応する受信機ｕ４に対する仮選択ラベルとして、

ＬＡＢＥＬ$_{1,3}$、ＬＡＢＥＬ$_{1,5}$、ＬＡＢＥＬ$_{1,8}$、ＬＡＢＥＬ$_{1,18}$、ＬＡＢＥＬ$_{2,5}$、ＬＡＢＥＬ$_{2,8}$、ＬＡＢＥＬ$_{2,18}$、ＬＡＢＥＬ$_{4,8}$、ＬＡＢＥＬ$_{4,18}$、ＬＡＢＥＬ$_{9,18}$、ＬＡＢＥＬ$_{1,\phi}$の１１個のラベルが選択される。

【０１６６】

管理センタ（ＴＣ）は、これらの仮選択ラベルの中から、受信機ｕｍに提供するラベルの再選択を行なう。なお、上記の１１個の仮選択ラベル中、ノードｉとノードｊが親子関係になっている第１の特別なサブセットＳＳ$_{i,j}$のラベルは、ＬＡＢＥＬ$_{1,3}$、ＬＡＢＥＬ$_{2,5}$、ＬＡＢＥＬ$_{4,8}$、ＬＡＢＥＬ$_{9,18}$の４つである。

【０１６７】

管理センタ（ＴＣ）は、これらの仮選択ラベルのうち、前述した第１および第２の特別なサブセットに対応するものを除外したラベルを受信機ｕ４に対する最終選択ラベルすなわち提供ラベルとする。

【０１６８】

さらに、管理センタ（ＴＣ）は、受信機に、その受信機が割り当てられているリーフ（葉）ｊの親ノードＰ（ｊ）を始点とし、ｊの兄弟ノードＳ（ｊ）に対応する特別なサブセットＳＳ$_{P(j),S(j)}$の中間ラベルＩＬ$_{P(j),S(j)}$を与える。上記の例では、管理センタ（ＴＣ）は、受信機ｕ４に、ＩＬ$_{9,18}$を与える。受信機は与えられたラベルと中間ラベルを
安全に保管する。

【０１６９】

すなわち、まず、受信機ｕ４が持つ必要のあるラベル（ＬＡＢＥＬ）として、ＬＡＢＥＬ$_{i,j}$のｉ，ｊの組を以下のものとしたラベルを仮選択ラベルとする。

ｉ＝１に対してｊ＝３，５，８，１８

ｉ＝２に対してｊ＝５，８，１８

ｉ＝４に対してｊ＝８，１８

ｉ＝９に対してｊ＝１８
リボークなしの場合用のＬＡＢＥＬを１つ
【０１７０】
次に、上記の１１個の仮選択ラベルから、前述した第１および第２の特別なサブセットに対応するものを除外したラベルと、１つの中間ラベルを受信機ｕ４に対する最終選択ラベルすなわち提供ラベルとする。すなわち、$ＬＡＢＥＬ_{i,j}$のｉ，ｊの組を以下のものとしたラベルを提供ラベルとする。
ｉ＝１に対してｊ＝５，８，１８
ｉ＝２に対してｊ＝８，１８
ｉ＝４に対してｊ＝１８
中間ラベル$ＩＬ_{9,18}$
以上、６つのラベルと１つの中間ラベルを提供ラベルとする。
【０１７１】
なお、上記例で示した受信機ｕ４以外の他の受信機ｕｍにおいても、与えられるラベルと中間ラベルの組み合わせは変わるものの、Ｎ＝１６の設定構成においては、各受信機ｕｍに対してそれぞれ６個のラベルと１個の中間ラベルが与えられる。
【０１７２】
なお、受信機ｕｍに対する提供ラベルとして設定される１つの中間ラベルは、階層木において、受信機ｕｍに最も近い祖先によって定義される第１の特別なサブセット、すなわち、ノードｉとノードｊが親子関係になっている第１の特別なサブセット$ＳＳ_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）に対応する中間ラベル$ＩＬ_{i,j}$となる。すなわち、階層木のリーフ（葉）対応の受信機に提供する１つの中間ラベルは、前述の第１特別サブセットを構成するサブセット$Ｓ_{i,j}$中、最下層の特別サブセットに対応する中間ラベルである。
【０１７３】
図２０に、上記のセットアップで、管理センタ（ＴＣ）が行う処理のフローを示す。まず、ステップＳ２０１において、階層木（ＨＫＴ）の構成を定義する。ステップＳ２０２において、設定した階層木に対応してサブセットの定義を行なう。サブセット定義は、必ずしも全てのリーフを個別にリボーク可能とする設定に限らず、配信情報に応じて、例えば特定のリーフの集合をまとめてリボーク単位としたサブセットなど、任意の設定が可能である。
【０１７４】
次に、ステップＳ２０３において、パラメータの設定、一方向性置換木の生成を行なう。ここでは、パラメータとして、葉（リーフ）の数＝Ｎ、ＲＳＡ暗号のパラメータである法Ｍ、秘密指数ｄを入力して、先に図１４のフローを参照して説明したアルゴリズムに従って葉がＮ個である２分木の一方向性置換木を生成し、各ノードｉの対応値$ｘ_{i}$を算出する。なお、ここで、各ノードｉの対応値$ｘ_{i}$の算出においては、前述の式（数式３）または式（数式４）のいずれかを適用する。
【０１７５】
ステップＳ２０４において、ノード対応値$ｘ_{i}$を中間ラベルの値として設定し、中間ラベル（ＩＬ）に基づいて、特別サブセット対応のラベルを算出する。すなわち、
$ＩＬ_{1,\phi}＝ｘ_{1}$
また、ｙ＝１，２，・・・，Ｎ－１に対して、
$ＩＬ_{y,2y}＝ｘ_{2y+1}$
$ＩＬ_{y,2y+1}＝ｘ_{2y}$
とする。
【０１７６】
なお、ここで求める中間ラベルは、
（ａ）リボークする受信機がひとつもない場合に使用する全受信機を含む第２の特別なサブセット$ＳＳ'_{1,\phi}$と、

（ｂ）ノードｉとノードｊが親子関係になっている第１の特別なサブセット$SS_{i,j}$（ただし、上述のようにｊ＝２，３，・・・，２Ｎ－１である）と、
に対応する中間ラベルである。
さらに、これらの中間ラベルに基づいて、特別サブセット対応のラベルを算出する。特別サブセット対応のラベルは、中間ラベルのハッシュ値によって算出される。

【０１７７】
次にステップＳ２０５において、特別サブセット対応のラベルに基づいて特別サブセット非対応のラベルを算出する。例えば、第１の特別なサブセット$SS_{i,j}$のラベル$LABEL_{i,j}$を擬似乱数生成器Ｇに入力し、ノードｉを始点とした、ノードｊの子ノードのラベル$LABEL_{i,LC(j)}$と、$LABEL_{i,RC(j)}$を求め、これらの処理を繰り返し実行して、設定したサブセット対応のラベルを全て算出する。

【０１７８】
次に、ステップＳ２０６においてパラメータを公開する。公開対象のパラメータは、例えば、ＲＳＡ暗号のパラメータである法Ｍ、公開指数ｅである。さらに、ステップＳ２０７において擬似乱数生成器関数Ｇと、ハッシュ関数Ｈを公開する。また、ステップＳ２０４で（数式４）を用いた場合にはハッシュ関数ｈも公開する。

【０１７９】
ステップＳ２０８において、階層木のリーフに対応して設定される各受信機へ提供するラベルおよび中間ラベルを選択する。この処理は、前述したように仮選択ラベルの選択と提供ラベルの選択の２段階処理として実行される。

【０１８０】
すなわち、まず、受信機ｕｍが持つ必要のあるラベル（ＬＡＢＥＬ）として，オリジナルのＳＤ方式において与えるラベル、すなわち受信機ｕｍが割り当てられたリーフ（葉）からルートに至るパスｍ（ｐａｔｈ－ｍ）上の内部ノードｉを始点とし、このリーフ（葉）からｉまでのパスから直接枝分かれしたノードｊに対応するサブセット$S_{i,j}$のラベル$LABEL_{i,j}$と、上記の第２の特別なサブセット$SS'_{1,\phi}$に対応するラベル$LABEL_{1,\phi}$を仮選択ラベルとして選択する。その後、仮選択ラベルから、前述した第１および第２の特別なサブセットに対応するものを除外したラベル$LABEL_{i,j}$と、１つの中間ラベルが提供ラベルとして設定される。

【０１８１】
なお、提供ラベルとして設定される１つの中間ラベルは、階層木において、受信機ｕｍが割り当てられた葉ｎの親ノードと兄弟ノードによって定義される第１の特別なサブセット、すなわち、ノードｉが葉ｎの親ノードであり，ノードｊが葉ｎの兄弟ノードであるような第１の特別なサブセット$SS_{i,j}$（ただし、ｊは葉であるためｊ＝Ｎ，Ｎ＋１，・・・，２Ｎ－１である）に対応する中間ラベル$IL_{i,j}$となる。例えば、図１９に示すノード番号１９の設定された受信機ｕ４に対して提供する中間ラベルは、中間ラベル$IL_{9,18}$となる。

【０１８２】
ステップＳ２０９において、ステップＳ２０８で決定した受信機に対する提供ラベルを受信機に提供し、処理を終了する。なお、ラベルの提供は、予め受信機の製造時に耐タンパ型のメモリに格納するか、あるいは、情報漏れの発生しないセキュアな通信路、あるいは媒体などの手段を適用して行なう。なお、図２０に示す処理フローの各ステップは、必ずしもこの順番である必要はない。

【０１８３】
（５－２）情報配信処理
次に、上述のセットアップ処理後に実行する秘密情報の送信処理の詳細について説明する。情報配信、すなわち秘密情報の送信は、管理センタ（ＴＣ）が１つ以上の暗号文を同報送信することによってなされる。それぞれの暗号文は、秘密情報をサブセットキーの１つを用いて暗号化したものである。例えば、管理センタが送信する秘密情報は、同じ送信秘密情報を異なるサブセットキーを用いて暗号化した複数の暗号文のセットとして構成さ

れる。

【０１８４】

例えば秘密情報を暗号化コンテンツの複合に適用する鍵：コンテンツキーＫｃとした場合、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のセットを生成して提供する。例えば、

Ｅ（$SK_{a,b}$，Ｋｃ），Ｅ（$SK_{c,d}$，Ｋｃ），Ｅ（$SK_{e,f}$，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。上記例は３つの異なるサブセットキーを適用して暗号化した３つの暗号文からなる暗号文セットである。

【０１８５】

サブセットキー$SK_{a,b}$、サブセットキー$SK_{c,d}$、サブセットキー$SK_{e,f}$のそれぞれは、特定の機器をリボーク機器として設定するために管理センタ（ＴＣ）において選択されたサブセットに対応するサブセットキーである。

【０１８６】

リボーク対象以外の受信機が、暗号文の暗号化に適用されたサブセットキーのいずれかを、受信機の保有するラベル（ラベルおよび中間ラベル）に基づいて生成可能であり、リボーク機器以外の正当な選択された受信機のみが、

Ｅ（$SK_{a,b}$，Ｋｃ），Ｅ（$SK_{c,d}$，Ｋｃ），Ｅ（$SK_{e,f}$，Ｋｃ）

に含まれるいずれかの暗号文の復号によってコンテンツキーＫｃを取得することができる。

【０１８７】

図２１に総受信機数Ｎ＝１６に設定した階層木構成において、受信機ｕ５，ｕ１１，ｕ１２をリボークする際に用いるサブセットを示す。受信機ｕ５，ｕ１１，ｕ１２をリボークする際に用いるサブセットは、図２１に示す２つのサブセット$S_{2,20}$と$S_{3,13}$である。

【０１８８】

リボークされない受信機は２つのサブセット$S_{2,20}$と$S_{3,13}$のいずれかに含まれ、リボークされる受信機ｕ５，ｕ１１，ｕ１２はそのいずれにも含まれないので、これらのサブセットに対応するサブセットキー$SK_{2,20}$と$SK_{3,13}$を用いて秘密情報を暗号化して送信すれば、リボークされない受信機のみが暗号文を復号して秘密情報を得ることができる。

【０１８９】

情報配信処理の処理手順について、図２２に示すフローを参照して説明する。図２２に示すフロー中の各ステップについて説明する。

【０１９０】

まず管理センタ（ＴＣ）は、ステップＳ３０１において、リボーク受信機、すなわち送信秘密情報の提供対象外とする排除機器を選択する。なお、すべての受信機は、階層木構成のリーフに対応して設定されている。

【０１９１】

次にステップＳ３０２において、決定したリボーク受信機に対応する階層木のリーフ位置に基づいて、秘密情報の配信名の際に適用するサブセットを決定する。例えば図２１の例では、リボーク受信機として受信機ｕ５，ｕ１１，ｕ１２を選択しており、適用するサブセットは２つのサブセット$S_{2,20}$と$S_{3,13}$となる。

【０１９２】

ステップＳ３０３において、決定したサブセットに対応するサブセットキーを選択する。管理センタ（ＴＣ）は、予めサブセットに対応するサブセットキーを保持している。例えば図２１の例では、２つのサブセット$S_{2,20}$と$S_{3,13}$とに対応する２つのサブセットキー$SK_{2,20}$と$SK_{3,13}$とが選択される。

【０１９３】

次に、ステップＳ３０４において、ステップＳ３０３で選択したサブセットキーを用い

て秘密情報を暗号化して暗号文セットを生成する。例えば図２１の例では、２つのサブセットキー$SK_{2,20}$と$SK_{3,13}$を用いて秘密情報を暗号化して暗号文セットを生成する。例えば図２１の例では、２つのサブセットキー$SK_{2,20}$と$SK_{3,13}$とを用いて秘密情報（例えばコンテンツキーＫｃ）を暗号化して、以下の暗号文セット、

$E(SK_{2,20}, Kc), E(SK_{3,13}, Kc)$

を生成する。

【０１９４】

ステップＳ３０５では、ステップＳ３０４において生成した暗号文セットを受信機に向けて送信（同報送信）する。送信される暗号文セットは、リボーク機器以外の受信機においてのみ復号可能な暗号文のみから構成され、リボーク機器においては復号できず、安全な情報配信が可能となる。

【０１９５】

なお、暗号文セットの送信に際しては、暗号文に含まれる各サブセット対応の暗号文の配列情報としてのサブセット指定情報を併せて送信してもよい。受信機は、この指定情報に基づいて、自装置で生成可能なサブセットキーを適用した暗号文を容易に抽出可能となる。この具体手な方式としては、例えば、特開２００１－３５２３２２号公報に示されている鍵指定コードを利用する構成が適用可能である。

【０１９６】

なお、暗号化に利用するサブセットキーは、管理センタ（ＴＣ）がセットアップフェイズにおいて作成して保管しておいたものを使用するようにしてもよいし、セットアップフェイズにおいて作成して保管しておいた各サブセットごとのラベルから擬似乱数生成器Ｇを用いて導出してもよい。

【０１９７】

また、セットアップフェイズにおいて$x_1$，Ｍ，ｄを保管しておき、これを用いてその都度必要なラベルおよびサブセットキーを導出してもよい。すなわち、サブセットキー生成処理として、管理センターから公開されている値である、値$x_1 \in Z^*_M$と、暗号パラメータとしての法Ｍおよび秘密指数ｄとを適用した落とし戸つき一方向性置換Ｆの逆置換$F^{-1}$を適用した演算式に基づいて、特別サブセットに対応する中間ラベルを算出し、中間ラベルに基づく演算処理により、特別サブセット対応のラベルを生成し、さらに該生成ラベルに基づく演算により特別サブセット非対応のラベルを生成するラベル生成し、これらのラベルに基づく演算処理によりサブセットキーを算出してサブセットキーを導出してもよい。

【０１９８】

なお、リボークする受信機がない場合には、前述の第２の特別なサブセット$SS'_{1,\phi}$のサブセットキー$SK_{1,\phi}$を用いて秘密情報の暗号化に用いる。

【０１９９】

（５－３）受信および復号処理

リボークされない受信機は、上記のサブセットのいずれかただ１つに属しているので、そのサブセットに対応するサブセットキーを用いて作られた暗号文を復号すれば秘密情報を得ることができる。受信機が復号すべき暗号文を見つけるためには、前述のサブセット指定情報を用いればよい。暗号文を特定した後、受信機は所有するラベルまたは中間ラベルからサブセットキーを導出し、これを用いて暗号文を復号する。サブセットキーを導出する方法を以下に述べる。

【０２００】

受信機ｕｍはまず、暗号文の復号処理に適用する求めるべきサブセットキー$SK_{i,j}$に対応するサブセット$S_{i,j}$のノードｊが、下記（Ａ），（Ｂ）のいずれであるかを判定する。

（Ａ）受信機が直接ラベル$LABEL_{i,k}$を持つノードｋの子孫である（ただしｊ＝ｋの場合を含む）か、

（Ｂ）ノードｉの子ノードのうち、受信機が割り当てられたリーフ（葉）ｎからルート

へのパス上にないほうのノード（つまり、パス上にあるノードｉの子ノードの兄弟であるノード）ｋと一致するかその子孫であるか、（すなわち、ノードｊが、ＳＤ方式において受信機ｕｍにラベルが与えられたサブセットのうち、第１の特別なサブセット$SS_{i,k}$を構成するノードｋの子孫であるか）を判断する。

【０２０１】

なお、リボークする受信機がなく、第２の特別なサブセット$SS'_{1,\phi}$のサブセットキー$SK_{1,\phi}$が秘密情報の暗号化に用いられている場合には（Ｂ）であるとみなす。

【０２０２】

（Ｂ）の場合には、下記のように、受信機に与えられている中間ラベル$IL_{P(n),S(n)}$から特別なサブセット$SS_{i,k}$の中間ラベルを導出する。

【０２０３】

まず、ｉ＝Ｐ（ｎ），ｊ＝ｋ＝Ｓ（ｎ）である場合には、受信機はすでにこの中間ラベルを持っているので特に何もする必要はない。そうでない場合は、受信機は中間ラベル$IL_{P(n),S(n)}$に対し公開されている置換関数Ｆ、すなわち落とし戸つき一方向性置換Ｆを適用することで、上位のサブセットに対応する中間ラベルを順次計算していく。受信機が持つ中間ラベル$IL_{P(n),S(n)}$に対し、受信機が割り当てられたリーフ（葉）ｎの親ノードＰ（ｎ）のさらに親ノードＰ（Ｐ（ｎ））を始点とし、ノードＰ（ｎ）の兄弟ノードＳ（Ｐ（ｎ））に対応する特別なサブセット$SS_{P(P(n)),S(P(n))}$の中間ラベル$IL_{P(P(n)),S(P(n))}$は、

$IL_{P(P(n)),S(P(n))} = ((IL_{P(n),S(n)})^{e} - n) \bmod M$

・・・（数式５）

によって求められる。

【０２０４】

これは、上述した一方向性置換木の性質に基づくものであり、ノード対応値算出において、前述の式（数式３）を適用した結果として、一方向性置換木の各ノード対応値ｘｉについて、下式が成立することに基づいている。

【数１５】

$$x_{\lfloor i/2 \rfloor} = (x_i^e - i) \bmod M$$

ただし、$\lfloor i \rfloor$は、ｉ以下の最大の整数を示す

【０２０５】

なお、一方向性置換木の生成時に、ノード対応値算出においてハッシュ関数を用いた前述の式（数式４）を適用した場合は、特別なサブセット$SS_{P(P(n)),S(P(n))}$の中間ラベル$IL_{P(P(n)),S(P(n))}$は、

$IL_{P(P(n)),S(P(n))} = ((IL_{P(n),S(n)})^{e} - h(n)) \bmod M$

・・・（数式６）

によって求められる。

【０２０６】

これらの出力にさらに公開パラメータとしてのＲＳＡ暗号における法Ｍ、公開指数ｅと

ノード番号ｉを用いた演算を繰り返していくことにより、受信機はサブセット$SS_{1,2}$または$SS_{1,3}$まで、ＳＤ方式において自身がラベルを保持すべきサブセットのうち第１の特別なサブセットのすべての中間ラベルを求めることができる。すなわち、あるノードｙとその親ノードＰ（ｙ）があるとき、ノードＰ（ｙ）の親ノードＰ（Ｐ（ｙ））を始点とし、ノードＰ（ｙ）の兄弟ノードＳ（Ｐ（ｙ））に対応する特別なサブセット$SS_{P(P(y)),S(P(y))}$の中間ラベル$IL_{P(P(y)),S(P(y))}$は、

$$IL_{P(P(y)),S(P(y))}=((IL_{P(y),S(y)})^{e}-y)\ mod\ M$$

・・・（数式７）

によって求められる。

【０２０７】

なお、一方向性置換木の生成時に、ノード対応値算出においてハッシュ関数を用いた前述の式（数式４）を適用した場合は、特別なサブセット$SS_{P(P(y)),S(P(y))}$の中間ラベル$IL_{P(P(y)),S(P(y))}$は、

$$IL_{P(P(y)),S(P(y))}=((IL_{P(y),S(y)})^{e}-h(y))\ mod\ M$$

・・・（数式８）

によって求められる。

【０２０８】

なおここで、ノードｙは受信機が割り当てられたリーフ（葉）からルートへのパス上に存在するノードである。

【０２０９】

また、中間ラベル$IL_{1,2}$、または、中間ラベル$IL_{1,3}$に対して、下式、

$$IL_{1,\phi}=((IL_{1,2})^{e}-3)\ mod\ M \quad \cdots（数式９）$$

$$IL_{1,\phi}=((IL_{1,3})^{e}-2)\ mod\ M \quad \cdots（数式１０）$$

によって、第２の特別なサブセット$SS'_{1,\phi}$に対応する中間ラベル$IL_{1,\phi}=K$を求めることができる。

【０２１０】

この場合も同様に、一方向性置換木の生成時に、ノード対応値算出においてハッシュ関数を用いた前述の式（数式４）を適用した場合は、中間ラベル$IL_{1,2}$、または、中間ラベル$IL_{1,3}$に対して、下式、

$$IL_{1,\phi}=((IL_{1,2})^{e}-h(3))\ mod\ M \quad \cdots（数式１１）$$

$$IL_{1,\phi}=((IL_{1,3})^{e}-h(2))\ mod\ M \quad \cdots（数式１２）$$

によって、第２の特別なサブセット$SS'_{1,\phi}$に対応する中間ラベル$IL_{1,\phi}=K$を求めることができる。

【０２１１】

受信機によって実行する具体的な中間ラベル取得処理について、図２１を参照して説明する。リーフ（葉）１９に割り当てられた受信機ｕ４は中間ラベル$IL_{9,18}$を保持している。公開パラメータとしてのＲＳＡ暗号における法Ｍ、公開指数ｅとノード番号ｉを用いた演算により、ノード９の親ノード４と兄弟ノード８で決定されるサブセット$S_{4,8}$の中間ラベル$IL_{4,8}$を、

$$IL_{4,8}=((IL_{9,18})^{e}-19)\ mod\ M$$

として求めることができる。

【０２１２】

同様に、ノード４の親ノード２と兄弟ノード５で決定されるサブセット$S_{2,5}$の中間ラベル$IL_{2,5}$を、

$$IL_{2,5}=((IL_{4,8})^{e}-9)\ mod\ M$$

として求めることができる。

【０２１３】

この処理を繰り返していくことにより、受信機ｕ４は、$IL_{1,3}$、および$IL_{1,\phi}$

を求めることができる。

【０２１４】

上記のようにして、サブセット$S_{i,k}$に対応する中間ラベル$IL_{i,k}$を導出したら、受信機はラベル$LABEL_{i,k}$を、

$LABEL_{i,k}=H(IL_{i,k})$として求める。

【０２１５】

それから、先に図７を用いて説明したように、擬似乱数生成器Ｇを用いて必要なサブセット$S_{i,j}$のラベル$LABEL_{i,j}$を求め、さらにそのサブセットのサブセットキー$SK_{i,j}$を

$SK_{i,j}=G_M(LABEL_{i,j})$

により求め、このサブセットキー$SK_{i,j}$を用いて暗号文を復号する。

【０２１６】

具体的なサブセットキーの導出処理例について、図２３を参照して説明する。図２３に示すように、受信機ｕ２，ｕ１１，ｕ１２がリボークされ、サブセット$S_{2,17}$およびサブセット$S_{3,13}$に対応するサブセットキーで暗号化された暗号文が同報配信されたとする。

【０２１７】

受信機ｕ４は、$LABEL_{1,5}$，$LABEL_{1,8}$，$LABEL_{1,18}$，$LABEL_{2,8}$，$LABEL_{2,18}$，$LABEL_{4,18}$，の６個のラベルと、$IL_{1,\phi}$，$IL_{1,3}$，$IL_{2,5}$，$IL_{4,8}$を導出できる中間ラベル$IL_{9,18}$を保持している。受信機ｕ４は上記の（Ａ）である。すなわち、受信機ｕ４はサブセット$S_{2,17}$に対し、ノード１７の先祖であるノード８を用いたラベル$LABEL_{2,8}$を直接保持しているため、これに擬似乱数生成器Ｇを必要な回数だけ適用することでサブセットキー$SK_{2,17}$を得ることができる。

【０２１８】

また、同じセッティングで、受信機ｕ５は、$LABEL_{1,4}$，$LABEL_{1,11}$，$LABEL_{1,21}$，$LABEL_{2,11}$，$LABEL_{2,21}$，$LABEL_{5,21}$の６個のラベルと、$IL_{1,\phi}$，$IL_{1,3}$，$IL_{2,4}$，$IL_{5,11}$を導出できる中間ラベル$IL_{10,21}$を保持している。受信機ｕ５は上記の（Ｂ）である。すなわち、受信機ｕ５はサブセット$S_{2,17}$に対し、ノード１７の先祖であるノードｋを用いたラベル$LABEL_{2,k}$を直接保持していない。このため、保持している中間ラベル$IL_{10,21}$から、ノード１７の先祖であるノード４に対応した中間ラベル$IL_{2,4}$を先に述べた手法でまず導出し、その後にラベル$LABEL_{2,4}$を求め、これに擬似乱数生成器Ｇを必要な回数だけ適用することでサブセットキー$SK_{2,17}$を得ることができる。

【０２１９】

もし、リボークすべき受信機が１台もなく、サブセットとして第２の特別なサブセット$SS'_{1,\phi}$が使用されていた場合、受信機ｕｍは、上記の処理により中間ラベル$IL_{1,\phi}$を求め、これを用いてラベル$LABEL_{1,\phi}$を、

ラベル$LABEL_{1,\phi}=H(IL_{1,\phi})$として計算し、

それを擬似乱数生成器Ｇに入力して出力の中央部分のＣビットを求める、すなわち、

$SK_{1,\phi}=G_M(LABEL_{1,\phi})$

によりサブセット$S_{1,\phi}$に対応するサブセットキー$SK_{1,\phi}$を求め、これを暗号文の復号に用いる。

【０２２０】

受信機によって実行する暗号文受領からサブセットキーの取得、復号処理の手順を図２４のフローチャートを参照して説明する。

【０２２１】

ステップＳ４０１において、まず受信機は、複数の暗号文からなる暗号文セットの中で自身が復号するものを決定する。これは、自身が生成可能なサブセットキーによって暗号化された暗号文を抽出する処理である。ここで、受信機が復号すべき暗号を決定できない

ということは、その受信機がリボークされていることを意味している。この暗号文選択処理は、例えば暗号文とともに送付されるサブセット指定情報に基づいて実行される。

【０２２２】

暗号文を決定したら、ステップＳ４０２において、受信機は、その暗号文の暗号化に用いられたサブセットキーを上記の手法で導出する。

【０２２３】

サブセットキーの導出処理の詳細手順について、図２５を参照して説明する。ステップＳ５０１において、受信機はまず、暗号文の復号処理に適用する求めるべきサブセットキー$SK_{i,j}$に対応するサブセット$S_{i,j}$のノードｊが、

（Ａ）受信機が直接ラベル$LABEL_{i,k}$を持つノードｋの子孫である（ただしｊ＝ｋの場合を含む）か、

（Ｂ）ノードｉの子ノードのうち、受信機が割り当てられたリーフ（葉）ｎからルートへのパス上にないほうのノード（つまり、パス上にあるノードｉの子ノードの兄弟であるノード）ｋと一致するかその子孫であるか（すなわち、ノードｊが、ＳＤ方式において受信機ｕｍにラベルが与えられたサブセットのうち、第１の特別なサブセット$SS_{i,k}$を構成するノードｋの子孫であるか）

を判断する。なお、リボークする受信機がなく、第２の特別なサブセット$SS'_{1,\phi}$のサブセットキー$SK_{1,\phi}$が秘密情報の暗号化に用いられている場合には、（Ｂ）であるとみなす。

【０２２４】

（Ａ）の場合には、ステップＳ５０３に進み、受信機が持つラベルに基づいて擬似乱数生成器Ｇを必要な回数適用して必要なサブセットキーを求める。

（Ｂ）の場合には、ステップＳ５０４に進み、受信機に与えられている中間ラベル$IL_{P(n),S(n)}$に基づいて、前述した式（数式５）または式（数式６）を適用して必要な特別サブセット対応の中間ラベルを算出する。さらに、ステップＳ５０５において、算出した中間ラベルのハッシュ計算によって、そのサブセットに対応するラベルＬＡＢＥＬを算出し、ステップＳ５０６において算出ラベルＬＡＢＥＬに基づいて擬似乱数生成器Ｇを適用して必要なサブセットキーを求める。

【０２２５】

図２４のフローに戻る。上記処理によってサブセットキーを導出した受信機は、ステップＳ４０４において、ステップＳ４０２で、暗号文セットから選択した暗号文を導出したサブセットキーで復号し、送信された秘密情報を得る。秘密情報はたとえばテレビ放送システムの暗号化コンテンツを復号するためのコンテンツキーであり、この場合には受信機は暗号化コンテンツを受信し、コンテンツキーを用いて復号して出力する。

【０２２６】

次に、図２６、図２７を参照してラベルの設定処理、暗号文の生成処理を実行する情報処理装置、および暗号文の復号処理を実行する受信機としての情報処理装置の機能構成について説明する。

【０２２７】

まず、図２６を参照してラベルの設定処理、暗号文の生成処理を実行する情報処理装置の構成について説明する。情報処理装置４１０は、中間ラベルおよびラベル生成手段４１１、提供ラベル決定手段４１２、暗号文生成手段４１３、暗号文提供手段４１４を有する。

【０２２８】

情報処理装置４１０は、階層木構成に基づくブロードキャストエンクリプション方式を適用し、排除（リボーク）機器を除く特定の選択機器にのみ復号可能とした暗号文の提供処理に適用する階層木を生成する情報処理装置であり、中間ラベルおよびラベル生成手段４１１は、階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、特別サブセットに対応するラベルの値を、中間ラベルに基づくハッシュ値として設定する。ハッシュ関数としては

、ＭＤ４またはＭＤ５またはＳＨＡ－１などが適用可能である。

【０２２９】

中間ラベルおよびラベル生成手段４１１において選択する特別サブセットは、

階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセットと、

階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセットと、

の少なくともいずれかである。

【０２３０】

中間ラベルおよびラベル生成手段４１１は、ＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、特別サブセットに対応するラベルをハッシュ関数Ｈにより導出可能とした中間ラベルを一方向性置換木のノード対応値として生成する。

【０２３１】

具体的には、先に図１４のフローを参照して説明したアルゴリズムに従ってＮ個の値：$x_N$～$x_{2N-1}$を決定しこれを中間ラベルとする。すなわち、末端ノード数Ｎの２分木構成を持つ階層木において、まず、数$x_1 \in Z^*_M$をランダムに選択し、ｉをカウンタとして、ｉ＝２～２Ｎ－１まで、ｉを１つずつ増加させながら、前述した式（数式３）または式（数式４）に従ってノード対応値$x_i$を算出して、Ｎ個の値：$x_N$～$x_{2N-1}$を決定し、このノード対応値$x_i$を、上述の第１特別サブセット$SS_{i,}$と、第２特別サブセット$SS'_{1,\phi}$のラベルを算出可能な中間ラベルとする。

【０２３２】

さらに、中間ラベルに基づくハッシュ算出により特別サブセットのラベルを算出し、その後、これらの特別サブセット対応のラベルに対して擬似乱数生成器Ｇを適用した演算により、順次各サブセット対応のラベルを算出する。これらの処理は、先に、図２０を参照して説明した処理である。

【０２３３】

提供ラベル決定手段４１２は、階層木の末端ノード対応の受信機に対する提供ラベルを決定する処理を実行する。提供ラベル決定手段４１２は、特別サブセットに対応しない特別サブセット非対応ラベルと、特別サブセットに対応するラベルを算出可能な中間ラベルとを受信機に対する提供ラベルとして決定する。

【０２３４】

提供ラベル決定手段４１２の具体的処理は以下の通りである。まず、受信機ｕｍが割り当てられたリーフ（葉）からルートに至るパスｍ（ｐａｔｈ－ｍ）上の内部ノードｉを始点とし、このリーフ（葉）からｉまでのパスから直接枝分かれしたノードｊに対応するサブセット$S_{i,j}$のラベル$LABEL_{i,j}$と、リボーク受信機がない場合に使用する全受信機を含む全体木に対応するサブセット$SS_{1,\phi}$に対応するラベル$LABEL_{1,\phi}$とを仮選択ラベルとし、この仮選択ラベルから特別サブセットに対応しない特別サブセット非対応ラベルを提供ラベルとし、さらに、特別サブセットに対応するラベルを算出可能な中間ラベルを選択して、これらを受信機ｕｍに対する最終提供ラベルとして決定する。

【０２３５】

暗号文生成手段４１３は、中間ラベルおよびラベル生成手段４１１の生成したラベルから導出可能なサブセットキーを選択的に適用して暗号化処理を実行して暗号文を生成する。暗号文提供手段４１４は、このようにして生成された暗号文をネットワークまたは媒体に格納して提供する。

【０２３６】

次に、図２７を参照して暗号文の復号処理を実行する受信機としての情報処理装置の機能構成について説明する。

【０２３７】

暗号文の復号処理を実行する受信機としての情報処理装置４２０は、暗号文選択手段４２１、ラベル算出手段４２２、サブセットキー生成手段４２３、復号手段４２４、ラベルメモリ４２５を有する。

【０２３８】

暗号文の復号処理を実行する受信機としての情報処理装置４２０は、階層木構成に基づくブロードキャストエンクリプション方式であるＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ）方式に基づいて設定するサブセット各々に対応するサブセットキーによって暗号化された暗号文の復号処理を実行する情報処理装置４２０であり、暗号文選択手段４２１は、処理対象の暗号文から、自己のラベルメモリ４２５に保持するラベル、または自己の保持する中間ラベルから算出可能なラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーを適用して生成した暗号文を選択する。

【０２３９】

ラベル算出手段４２２は、暗号文の適用サブセットキーが、保持ラベルに基づく擬似乱数生成処理によって導出可能なサブセットキーでない場合に、受信機に与えられている中間ラベル$IL_{P(n),S(n)}$に基づく演算処理を実行して、必要な特別サブセット対応の中間ラベルを算出する。

【０２４０】

具体的には、受信機に与えられ、ラベルメモリ４２５に格納されている中間ラベル$IL_{P(n),S(n)}$に基づいて、前述した式（数式５）または式（数式６）を適用して必要な特別サブセット対応の中間ラベルを算出する。さらに、算出した中間ラベルのハッシュ計算によって、そのサブセットに対応するラベルＬＡＢＥＬを算出する。

【０２４１】

サブセットキー生成手段４２３は、ラベルメモリ４２５に格納されているラベル、あるいは、ラベル算出手段４２２において中間ラベルから算出されたラベルＬＡＢＥＬに基づいて擬似乱数生成器Ｇを適用して必要なサブセットキーを求める。

【０２４２】

復号手段４２４は、サブセットキー生成手段４２３において算出したサブセットキーに基づいて、暗号文の復号処理を実行する。

【０２４３】

図２８に、ラベルの設定処理、暗号文生成処理を実行する情報処理装置、および暗号文復号処理を実行する受信機としての情報処理装置５００のハードウェア構成例を示す。図中で点線で囲われたブロックは必ずしも備わっているわけではない。たとえばメディアインタフェース５０７は、受信機５００が光ディスクプレーヤ等である場合に装備する。入出力インタフェース５０３は、受信機５００が他の機器と情報のやりとりをしたり、アンテナからの信号を受信したりする場合に装備される。重要なのは、セキュア記憶部５０４であり、セットアップフェイズにおいて、管理センタ（ＴＣ）から与えられたラベルが安全に保管される。

【０２４４】

情報処理装置５００は、図２８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。

【０２４５】

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部および暗号処理部として機能する。ラベルおよび中間ラベルの算出処理、ラベルに基づくサブセットキー算出処理を実行する。さらに、情報処理装置５００が受信機としての情報処理装置である場合、サブセットキーに基づく暗号文の復号処理を実行する。

【０２４６】

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。

【０２４７】

情報処理装置５００が受信機としての情報処理装置である場合、セキュア記憶部５０４に、例えばセットアップフェイズにおいて、管理センタ（ＴＣ）から与えられたラベル、中間ラベル、各種ＩＤなど、安全にまたは秘密に保持すべきデータが保存される。

【０２４８】

セキュア記憶部５０４には、サブセットから選択された特別サブセット対応のラベル（ＬＡＢＥＬ）を生成可能な中間ラベルと、特別サブセット非対応のラベル（ＬＡＢＥＬ）とが格納される。

【０２４９】

情報処理装置５００が受信機としての情報処理装置である場合、セキュア記憶部５０４に格納される中間ラベルに基づいて生成されるラベルは、特別サブセット対応のラベル（ＬＡＢＥＬ）であり、具体的には、

（ａ）階層木において、ノードｉを頂点とする部分木からノードｉより下層のノードｊを頂点とする部分木を除く集合として定義されたサブセット$S_{i,j}$中、ノードｉおよびノードｊが階層木において直結された親子関係にある第１特別サブセット、

（ｂ）階層木のすべてのリーフを含むルートを頂点とする全体木の集合として定義されたサブセット$S_{1,\phi}$である第２特別サブセット、

上記（ａ），（ｂ）の特別サブセット対応のラベルである。

【０２５０】

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。ディスプレイ装置５０６は復号コンテンツの出力等に利用される。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。

【０２５１】

［６．Ｂａｓｉｃ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（ベーシックＬＳＤ）方式の概要］

次に、Ｂａｓｉｃ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（ベーシックＬＳＤ）方式の概要について説明する。

【０２５２】

前述の背景技術の欄で説明した［非特許文献２： Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｇｒａｐｈｙ－Ｃｒｙｐｔｏ ２００２, Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ ２４４２, Ｓｐｒｉｎｇｅｒ, ２００２, ｐｐ４７－６０「Ｄ．Ｈａｌｅｖｙ ａｎｄ Ａ．Ｓｈａｍｉｒ著"Ｔｈｅ ＬＳＤ Ｂｒｏａｄｃａｓｔ Ｅｎｃｒｙｐｔｉｏｎ Ｓｃｈｅｍｅ"」］には、ＳＤ方式を改良したＬａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ方式が提案されている。ＬＳＤ方式には、Ｂａｓｉｃ（基本）方式と、その拡張であるＧｅｎｅｒａｌ（一般化）方式がある。ここではＢａｓｉｃ方式について説明する。

【０２５３】

ＬＳＤ方式はＳＤ方式の拡張であり、レイヤという新たな概念を取り入れたものである。ＳＤ方式における木構造の中で、特定の高さを特別レベル（Ｓｐｅｃｉａｌ Ｌｅｖｅｌ）として定義する。ベーシックＬＳＤ方式においては特別レベルは、１種類だけであるが、一般化ＬＳＤ方式においては重要度の異なる複数の特別レベルを用いる。

【０２５４】

いま、簡単のため、$\log^{1/2}N$を整数であるとする。ベーシックＬＳＤ方式では、図２９に示すように、木のルートからリーフ（葉）に至るまでのそれぞれのレベル（階）のうち、ルートとリーフ（葉）のレベルを含む$\log^{1/2}N$ごとのレベルを特別レベル

であると決める。そして、隣り合う２つの特別レベルに挟まれた階層（両端の特別レベルを含む）を、レイヤと呼ぶ。図２９の例では、ルートのレベル、ノードｋを含むレベル、リーフ（葉）のレベルが特別レベルであり、ルートのレベルとノードｉを含むレベルとノードｋを含むレベルが１つのレイヤを構成する。またノードｋを含むレベルとノードｊを含むレベルとリーフ（葉）を含むレベルが別のレイヤを構成する。

【０２５５】

ベーシックＬＳＤ方式においては、ＳＤ方式において定義されたサブセット$S_{i,j}$のうち、（１）ノードｉとノードｊが同一レイヤにあるか、もしくは（２）ノードｉが特別レベルにあるか，少なくとも一方の条件を満たすものだけを定義する。このようにすると、ＳＤ方式において用いられたサブセットのうちのいくつかはベーシックＬＳＤ方式では定義されなくなってしまうが、このサブセットはベーシックＬＳＤ方式で定義されたサブセットの高々２つの和集合で表すことができる。たとえば図２９の例では、サブセット$S_{i,j}$は、ベーシックＬＳＤ方式では定義されないが、ノードｉからノードｊへのパス上の、ノードｉに最も近い特別レベル上のノード（ノードｋ）を用いて、

$S_{i,j} = S_{i,k} \cup S_{k,j}$

と表すことができる。

【０２５６】

つまり、ＳＤ方式においてはサブセット$S_{i,k}$に対応するサブセットキー$SK_{i,k}$を用いて暗号化した１つの暗号文の代わりに、ベーシックＬＳＤ方式においてはサブセット$S_{i,k}$と$S_{k,j}$に対応するサブセットキー$SK_{i,k}$と$SK_{k,j}$を用いて暗号化した２つの暗号文を送信する。

【０２５７】

この工夫により、送信される暗号文の数はＳＤ方式の高々２倍に増加するのみであり、一方、各受信機が保持するラベルの数は、上述したＳＤ方式よりも減らすことができる。

【０２５８】

先に図９を参照して、ＳＤ方式において各受信機が保持するラベルの数の説明を行なったが、同じセッティングの場合のベーシックＬＳＤ方式における各受信機が保持するラベルの数について、図３０を参照して説明する。図３０中の受信機ｕ４は、ｉ，ｊが同一レイヤにあるか、ｉが特別レベルにあるラベル$LABEL_{i,j}$のみ保持しておけばよい。すなわち、受信機ｕ４が保持するラベルは、$LABEL_{1,3}$，$LABEL_{1,5}$，$LABEL_{1,8}$，$LABEL_{1,18}$，$LABEL_{2,5}$，$LABEL_{4,8}$，$LABEL_{4,18}$，$LABEL_{9,18}$となる。さらに、ＳＤ方式と同様に、リボークする受信機がない場合に用いる特別なラベルも保持する必要がある。

【０２５９】

総受信機数をＮとしたときに、各受信機が保持しておくラベルの総数は下記のように求められる。まず、レイヤ１つあたりのラベル数は、ノードｉを決めるとラベル内でのｉの高さ分だけノードｊが存在するので、下式によって算出される数となる。

【数１６】

$$\sum_{i=1}^{\log^{1/2} N} i = \frac{1}{2}(\log N + \log^{1/2} N)$$

となる。

【０２６０】

階層木にレイヤは、ｌｏｇ$^{1/2}$Ｎ個あるから、階層木全体のレイヤでのラベル数は下式によって算出される数となる。

【数１７】

$$\frac{1}{2}(\log^{3/2} N + \log N)$$

である。

【０２６１】

次にノードｉが特別レベルであるものを考えると、階層木全体におけるｉの高さ分だけノードｊが存在するので、ノードｉが特別レベルであるものを含む階層木全体のラベル数は下式によって算出される数となる。

【数１８】

$$\sum_{i=1}^{\log^{1/2} N} (\log^{1/2} N)i = \frac{1}{2}(\log^{3/2} N + \log N)$$

である。

【０２６２】

いま、ノードｉが特別レベルにあり、ノードｊが同一レイヤにあるものは重複して数えたので、その分を引く必要がある。この組み合わせは、１つのレイヤにつきｌｏｇ$^{1/2}$Ｎ個あるので全体ではｌｏｇＮ個である。これらと、リボークする受信機がない場合のための特別な１つを加えると、ベーシックＬＳＤ方式において各受信機が保持するラベルの総数は、下式によって与えられる数となる。

【数１９】

$$\frac{1}{2}(\log^{3/2} N+\log N)+\frac{1}{2}(\log^{3/2} N+\log N)-\log N+1=\log^{3/2} N+1$$

である。

【０２６３】

［７．一方向性置換木を用いたベーシックＬＳＤ方式のラベル数削減構成］

次に、一方向性置換木を用いたベーシックＬＳＤ方式のラベル数削減構成について説明する。前述のＳＤ方式を基にした本発明では、ノードｉがノードｊの親である場合のサブセット$S_{i,j}$のラベル$LABEL_{i,j}$を求めるための中間ラベル$IL_{i,j}$を導出できる特定の中間ラベルを１つだけ持つようにすることで、各受信機が持つラベルの数を減らした。この手法は、ベーシックＬＳＤ方式についても同様に適用することができる。

【０２６４】

具体的な構成方法は、前述の本発明の実施例とほぼ同じである。ただ、セットアップ時に、管理センタ（ＴＣ）が擬似乱数生成器Ｇを用いてラベル$LABEL_{i,j}$を次々と作成していく際に、ノードｉが特別レベルにない場合、ｉの直下の特別レベルよりも下のノードをｊとするラベルは利用されないので、その特別レベルまででラベルの生成を止めることができる。また、作られたラベルを各受信機に配布する際も、上述の条件を満たすラベルのみが作成されているので、それだけを受信機に配布すればよい。

【０２６５】

図３０を参照して説明したと同様のセッティングとして、一方向性置換木を用いたベーシックＬＳＤ方式のラベル数削減構成の具体例を図３１を参照して説明する。ベーシックＬＳＤ方式において、受信機ｕ４が保持するラベルは、図３０を参照して説明したように、$LABEL_{1,3}$，$LABEL_{1,5}$，$LABEL_{1,8}$，$LABEL_{1,18}$，$LABEL_{2,5}$，$LABEL_{4,8}$，$LABEL_{4,18}$，$LABEL_{9,18}$と、さらに、ＳＤ方式と同様の、リボークする受信機がない場合に用いる特別なラベルの合計９個のラベルを保持しておく必要があった。これに対し、本発明のようにノードｉ，ｊが親子関係となるものと、リボークする受信機がない場合に使われる特別なサブセットに対応する中間ラベル$IL_{i,j}$および$IL_{1,\phi}$を導出できる中間ラベル$IL_{9,18}$を持つようにすると、４個のラベル$LABEL_{1,5}$，$LABEL_{1,8}$，$LABEL_{1,18}$，$LABEL_{4,18}$と、１つのと中間ラベル$IL_{9,18}$の合計５個を保持すればよい。

【０２６６】

総受信機数をＮとした場合に本発明により削減できるラベルの個数を考える。本発明を適用しないベーシックＬＳＤ方式において、ノードｉ，ｊが親子関係になるようなラベル$LABEL_{i,j}$を各受信機がいくつ保持すべきかを考える。

【０２６７】

ノードｉ，ｊが親子関係になっているときには、以下の３つの場合が考えられる。

（Ａ）ノードｉが特別レベルにある。

（Ｂ）ノードｊが特別レベルにある。
（Ｃ）ノードｉもｊも特別レベルにない。
これらのいずれの場合も、ノードｉ，ｊが親子関係にある（つまり、隣り合っている）場合には、ｉとｊは同一レイヤに存在する。すなわち、サブセット$Ｓ_{ｉ，ｊ}$はベーシックＬＳＤ方式で定義されるための条件を満たしている。つまり、このようなサブセットはベーシックＬＳＤ方式で定義され使用されるため、受信機はそれに対応する$ＬＥＢＥＬ_{ｉ，ｊ}$を保持しておく必要がある。

【０２６８】
ある受信機に対してこのようなノードｉ，ｊは、ｉの取り方が木の高さ分（すなわち、受信機が割り当てられたリーフ（葉）からルートへのパス上の、リーフ（葉）を除くノードすべて）あり、ｉを決めればｊがただ１つ決まる（ｉの子で、上記のパス上にないノード）ため、木の高さ分、すなわちｌｏｇＮ個だけ存在する。

【０２６９】
本発明を用いて、これらのｌｏｇＮ個のラベルと１つの特別なラベルを、１つの中間ラベルから作り出すようにすることにより、受信機が保持するラベルの数を、
ｌｏｇＮ＋１－１＝ｌｏｇＮ
だけ削減することが可能となる。

【０２７０】
上述のように、ベーシックＬＳＤ方式では受信機が保持するラベルの総数は、
$ｌｏｇ^{３／２}Ｎ＋１$
であったため、本発明を適用することによりこれを、
$ｌｏｇ^{３／２}Ｎ－ｌｏｇＮ＋１$
に削減することができる。

【０２７１】
［８．Ｇｅｎｅｒａｌ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（一般化ＬＳＤ）方式の概要］
次に、Ｇｅｎｅｒａｌ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（一般化ＬＳＤ）方式の概要について説明する。

【０２７２】
ベーシックＬＳＤ方式では、１種類の特別レベルを用いていたが、Ｇｅｎｅｒａｌ Ｌａｙｅｒｅｄ Ｓｕｂｓｅｔ Ｄｉｆｆｅｒｅｎｃｅ（一般化ＬＳＤ）方式では、重要度の異なる複数の特別レベルを用いる。

【０２７３】
ＬＳＤ方式を提案した論文と同様に、階層木において、ルートからノードｉを経てノードｊに至るパスを１本のグラフとして考える。木のルートとノードｊが端点となり、木のノードがグラフのノードとなり、端点以外のノードのひとつがノードｉとなっている。このグラフでは、各ノードはルートからの距離で表される。この距離は、ｄ桁のｂ進数（ただしｂ＝$（ｌｏｇ^{１／ｄ}Ｎ）$）で表される。たとえば、ルートは０...００と表され、その隣のノード（階層木構造で、ルートの子ノードであるノード）は０...０１と表される。

【０２７４】
$サブセットＳ_{ｉ，ｊ}$は、定義された変換（ノードからノードへの遷移）を組み合わせての、ノードｉからノードｊへの最終的な遷移であると考える。定義された変換は定義されたサブセットを表し、最終的な遷移に要する個々の遷移が、$サブセットＳ_{ｉ，ｊ}$を分割して表すのに必要な定義されたサブセットを示す。もとの論文にあるように、ノードｉ，$ｋ_{１}$，$ｋ_{２}$，・・・，$ｋ_{ｄ－１}$，ｊがこの順で木のパス上に存在するときには、ＳＤ方式におけるサブセット$Ｓ_{ｉ，ｊ}$は一般化ＬＳＤ方式においては、下式によって示される。

【数２０】

$$S_{i,j} = S_{i,k_1} \cup S_{k_1,k_2} \cup \cdots \cup S_{k_{d-1},j}$$

【０２７５】
すなわち、ＳＤ方式におけるサブセットＳ$_{i,j}$は一般化ＬＳＤ方式においては、高々ｄ個のサブセットの和集合で表される。
【０２７６】
一般化ＬＳＤ方式では、ノードｉが上記のグラフで［ｘ］（→）ａ［０］（→）（ただしａは非ゼロの数字のうち一番右にある数字、［ｘ］（→）は任意の数字列、［０］（→）はゼロの列である）と表されるとき、［ｘ＋１］（→）０［０］（→）、もしくは、［ｘ］（→）ａ'［ｙ］（→）（ただしａ'＞ａであり、［ｙ］（→）は［０］（→）と同じ長さの任意の数字列）のいずれかで表されるノードｊへの遷移をすべて定義する。すなわち，そのようなｉ，ｊの組で表されるサブセットＳ$_{i,j}$をすべて定義する．
【０２７７】
このようにすると、ベーシックＬＳＤ方式は、一般化ＬＳＤ方式においてｄ＝２で、（一番右の）最終桁が０である２桁の数字で表されるレベルが特別レベルであるものと考えることができる。一般化ＬＳＤ方式では、ノードｉを表す数字における一番右のゼロの列の桁数が、そのレベルの重要度を表し、ノードｊはｉ＋１からｉよりも重要度の高い最初のノードまでのいずれのノード（両端のノードを含む）にもなる可能性がある。このようなセッティングで、たとえばｉ＝８２５９１７，ｊ＝８６４５６３とすると、ｉからｊへの遷移、すなわちＳＤ方式におけるサブセットＳ$_{i,j}$は、
８２５９１７→８２５９２０→８２６０００→８３００００→８６４５６３
という一般化ＬＳＤ方式で定義された４つの遷移によって表すことができる。
【０２７８】
すなわち、ｋ$_1$＝８２５９２０，ｋ$_2$＝８２６０００，ｋ$_3$＝８３００００とおけば、サブセットＳ$_{i,j}$は下式によって示される。すなわち、
【数２１】

$$S_{i,j} = S_{i,k_1} \cup S_{k_1,k_2} \cup S_{k_2,k_3} \cup S_{k_3,j}$$

となる。
【０２７９】
ＳＤ方式の上記のサブセットＳ$_{i,j}$に属する受信機に秘密情報を伝送するためには、一般化ＬＳＤ方式においては、下式によって示されるサブセット、

【数２２】

$$S_{i,k_1}, S_{k_1,k_2}, S_{k_2,k_3}, S_{k_3,j}$$

に対応するサブセットキーで暗号化した４つの暗号文を送信する。

【０２８０】

一般化ＬＳＤ方式で各受信機が保持すべきラベル数は、パラメータｄを大きくしていくことにより減少していき、最終的には、

Ｏ（ｌｏｇ$^{1+\varepsilon}$Ｎ）

を得る。ただしε＝１／ｄである。またこのとき、送信すべき暗号文数の上限は、

ｄ（２ｒ－１）

となる。詳細については上記の論文を参照されたい。

【０２８１】

［９．一方向性置換木を用いた一般化ＬＳＤ方式のラベル数削減構成］

次に、一方向性置換木を用いた一般化ＬＳＤ方式のラベル数削減構成について説明する。前述の、ベーシックＬＳＤ方式に一方向性置換木を用いて受信機が保持すべきラベル数を削減する手法は、一般化ＬＳＤ方式についても適用できる。具体的には、ベーシックＬＳＤ方式と一般化ＬＳＤ方式は定義されるサブセットが満たすべき条件が違うのみであり、一方向性置換木を利用する部分に違いはない。

【０２８２】

一般化ＬＳＤ方式においても、受信機ｕｍは、ＳＤ方式において定義され受信機ｕｍに与えられるラベルのうち、ノードｉ，ｊが親子関係になっているサブセット$S_{i,j}$に対応するラベル$LABEL_{i,j}$をすべて保持しておく必要がある。これは、ノードｉとしてどんな値をとっても、その子ノードｊ（すなわちｉ＋１）への遷移は、上述の定義される遷移の条件に当てはまるためである。すなわち、ベーシックＬＳＤ方式と同様に、ある受信機にとって、保持すべきラベルのうちノードｉ，ｊが親子関係になっているものはｌｏｇＮ個ある。これらのラベルと特別なラベルを１つの中間ラベルから作り出すようにすることにより、ｌｏｇＮ個のラベルの削減が可能となる。もともと一般化ＬＳＤ方式で各受信機が保持しておくべきラベルの数は、

Ｏ（ｌｏｇ$^{1+\varepsilon}$Ｎ）

（ただしεは任意の正数）であったため、ここからｌｏｇＮ個のラベルを削減できることになる。

【０２８３】

もともと一般化ＬＳＤ方式で各受信機が保持しておくべきラベルの数は、ＳＤ方式やベーシックＬＳＤ方式に比較すると少ない設定であり、この設定からさらにＳＤ方式やベーシックＬＳＤ方式と同様の数のラベル数削減が可能となる意味で、削減の効果がさらに顕著となる。

【０２８４】

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。

【０２８５】

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。

【０２８６】

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－ＲＯＭ(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エアとして提供することができる。

【０２８７】

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。

【０２８８】

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。

【産業上の利用可能性】

【０２８９】

以上、説明したように、本発明の構成によれば、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情報配信構成において比較的に効率的な構成であるとされているＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式、およびＬａｙｅｒｅｄ　Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＬＳＤ）方式に対して、さらに１つの落とし戸つき一方向性置換に基づく一方向性置換木を適用することにより、各受信機（情報処理装置）が安全に保持すべき情報量を削減することが可能となる。

【０２９０】

さらに、本発明の構成においては、ＳＤ方式やＬＳＤ方式に基づいて設定するサブセット各々に対応するラベル（ＬＡＢＥＬ）中、選択された一部の特別サブセットに対応するラベルの値を演算処理により算出可能な値として設定した中間ラベル（ＩＬ）を生成し、この中間ラベルについて、少なくとも１つの中間ラベルの値に基づく落とし戸つき一方向性置換Ｆの適用により他の中間ラベルの値を算出可能な値を持つ構成とした。受信機には、特別サブセット非対応のラベルに加えて、特別サブセット対応のラベルを導出可能な１つの中間ラベルのみを提供する構成としたので、従来のＳＤ方式やＬＳＤ方式において受信機に提供されるラベルの数を、削減することが可能となる。削減したラベルについては、受信機側で保持する中間ラベルに対する落とし戸つき一方向性置換Ｆの実行により他の中間ラベルを算出可能であり、従来のＳＤ方式やＬＳＤ方式に基づいて設定可能なサブセットの全てに対応する処理が可能である。このように本発明の構成を適用することにより、各受信機が安全に保持すべき情報量（ラベル）の削減が実現する。

【図面の簡単な説明】

【０２９１】

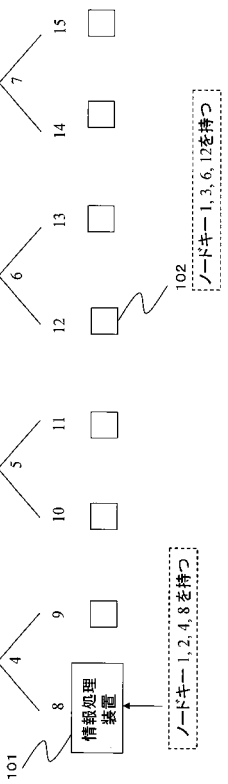
【図１】２分木階層型木構造について説明する図である。

【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。

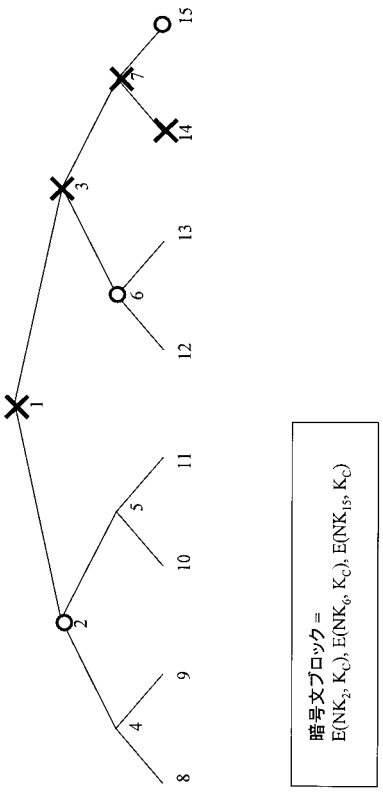
【図３】Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式において適用するノードが２つに分岐する階層型木構造を説明する図である。
【図４】Ｃｏｍｐｌｅｔｅ　Ｓｕｂｔｒｅｅ（ＣＳ）方式においてリーフ対応の受信機の持つノードキーについて説明する図である。
【図５】ＣＳ方式において秘密情報をリボークされない受信機のみに選択的に提供するかについて説明する図である。
【図６】Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式におけるサブセットの定義について説明する図である。
【図７】Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式におけるラベルの設定および構成について説明する図である。
【図８】Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式におけるサブセットの設定について説明する図である。
【図９】ＳＤ方式において、全受信機数Ｎ＝１６の設定の場合に各受信機が保持すべきラベルを示す図である。
【図１０】ＳＤ方式において、各受信機が保持すべきラベルの詳細について説明する図である。
【図１１】ＳＤ方式において、各受信機が保持すべきラベルの詳細について説明する図である。
【図１２】ＳＤ方式において、特定の受信機ｕ４が属するサブセットの詳細について説明する図である。
【図１３】一方向性置換木の構成について説明する図である。
【図１４】一方向性置換木のノードに対応する２Ｎ－１個のノード対応値を設定するアルゴリズムを説明するフロー図である。
【図１５】ルートを１とし、以下、下層ノードについて順次、幅優先（ｂｒｅａｄｔｈ　ｆｉｒｓｔ　ｏｒｄｅｒ）で、識別子（番号）を付与したノード番号設定例について説明する図である。
【図１６】ノードが親子関係になっている第１の特別なサブセット$SS_{P(y),S(y)}$の構成例について説明する図である。
【図１７】特別なサブセット対応のラベルと、図１４を参照して説明したアルゴリズムによって算出した２Ｎ－１個の中間ラベルとして利用される値$x_1, x_2, \ldots, x_{2N-1}$との対応を示す図である。
【図１８】図１６に対応するサブセットにおける中間ラベル、ラベルの対応について説明する図である。
【図１９】受信機に提供するラベルの決定処理について説明する図である。
【図２０】セットアップ処理のフローを示す図である。
【図２１】総受信機数Ｎ＝１６に設定した階層木構成において、受信機ｕ５，ｕ１１，ｕ１２をリボークする際に用いるサブセットを示す図である。
【図２２】情報配信処理の処理手順について説明するフローを示す図である。
【図２３】具体的なサブセットキーの導出処理例について説明する図である。
【図２４】受信機によって実行する暗号文受領からサブセットキーの取得、復号処理の手順を説明するフローチャートを示す図である。
【図２５】一方向性置換木を適用したＳＤ方式において、受信機におけるサブセットキー導出処理の詳細手順について説明するフロー図である。
【図２６】ラベルの決定処理、暗号文の生成処理を実行する情報処理装置の構成について説明する図である。
【図２７】暗号文の復号処理を実行する受信機としての情報処理装置の機能構成について説明する図である。
【図２８】情報処理装置のハードウェア構成例としてのブロック図を示す図である。
【図２９】ベーシックＬＳＤ方式について説明する図である。
【図３０】ベーシックＬＳＤ方式における各受信機が保持するラベルの数について説明す

る図である。
【図３１】一方向性置換木を用いたベーシックＬＳＤ方式のラベル数削減構成について説明する図である。
【符号の説明】
【０２９２】
１０１　情報処理装置
２０１　ノード
２３１，２３２　ノード
２５１　リーフ
３０１　ノード
３０２　親ノードＰ（ｉ）
３０３　兄弟ノードＳ（ｉ）
３１０　サブセットＳＳ$_{P(y),S(y)}$
４１０　情報処理装置
４１１　中間ラベルおよびラベル生成手段
４１２　提供ラベル決定手段
４１３　暗号文生成手段
４１４　暗号文提供手段
４２０　情報処理装置
４２１　暗号文選択手段
４２２　ラベル算出手段
４２３　復号手段
４２４　ラベルメモリ
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
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

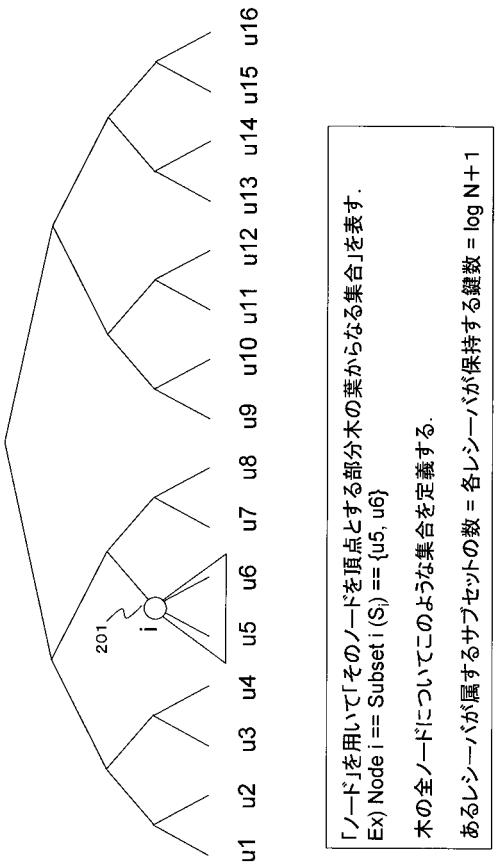
【図１】


情報処理装置
101
102
ノードキー 1, 2, 4, 8 を持つ
ノードキー 1, 3, 6, 12を持つ

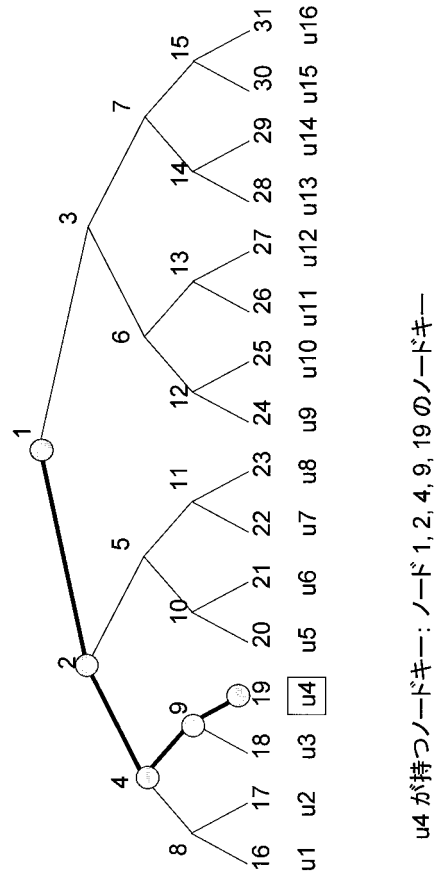
【図２】


暗号文ブロック＝
E(NK2, KC), E(NK6, KC), E(NK15, KC)

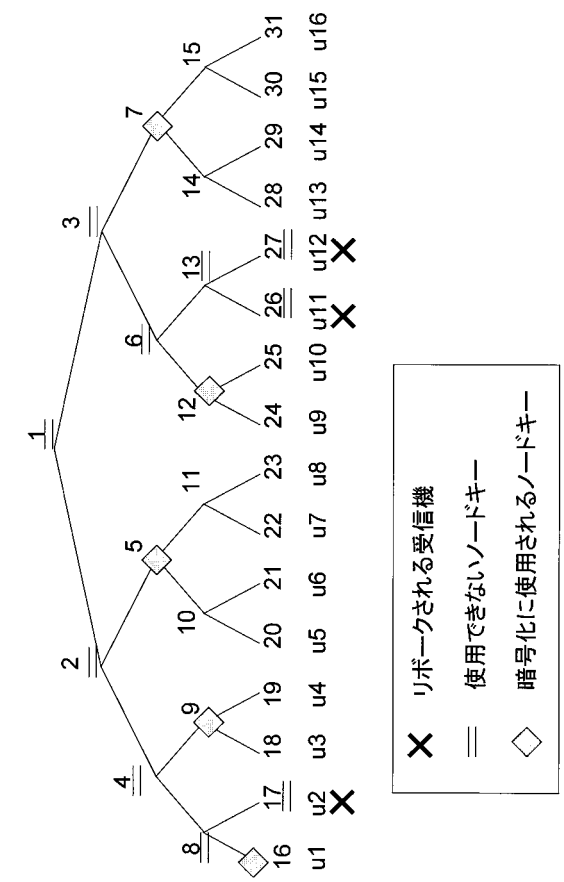
【図３】


u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16
201
i
「ノード」を用いて「そのノードを頂点とする部分木の葉からなる集合」を表す.
Ex) Node i == Subset i (Si) == {u5, u6}
木の全ノードについてこのような集合を定義する.
あるレシーバが属するサブセットの数 = 各レシーバが保持する鍵数 = log N+1

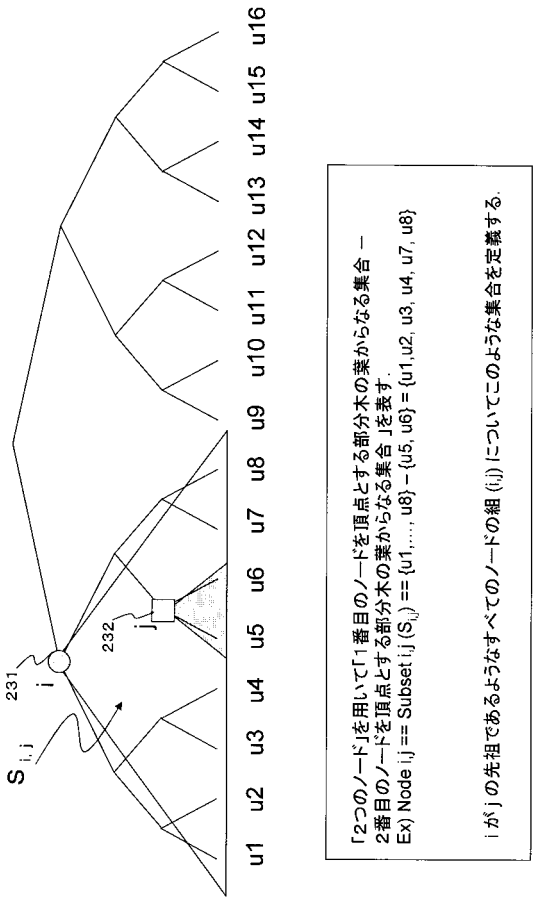
【図４】


u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16
u4 が持つノードキー: ノード 1, 2, 4, 9, 19 のノードキー

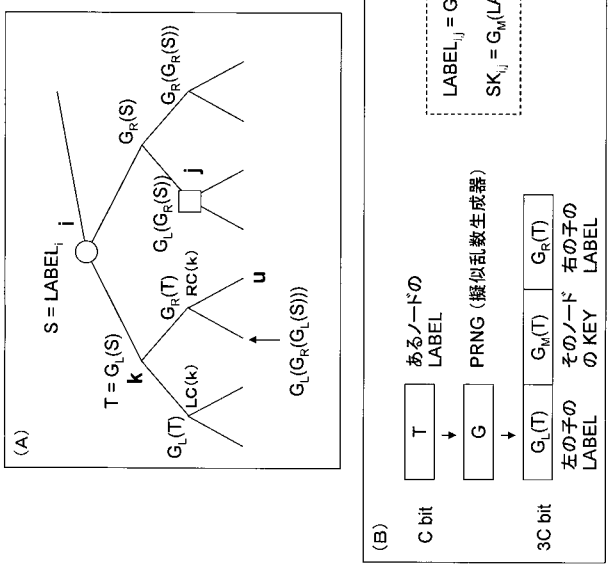
【図５】


リボークされる受信機
使用できないノードキー
暗号化に使用されるノードキー
u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16

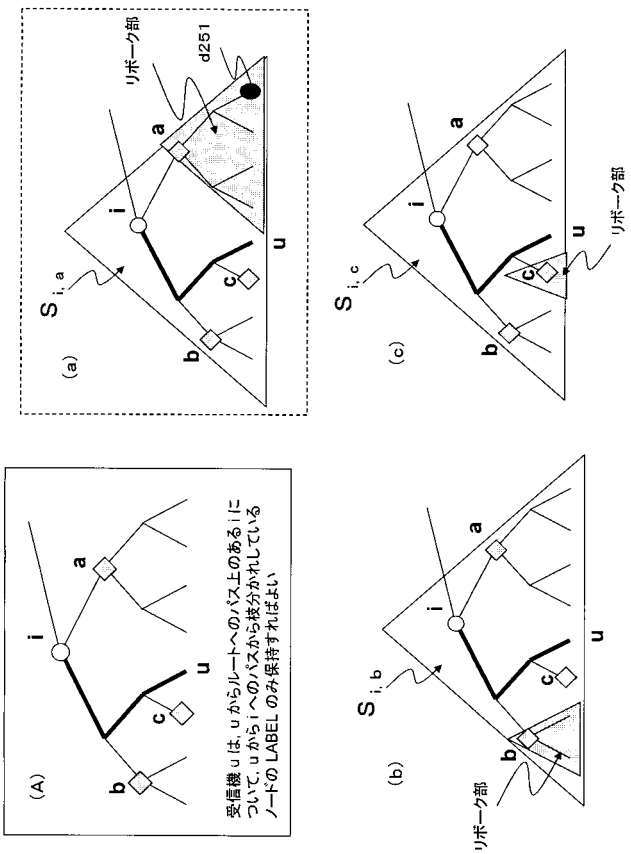
【図６】


「2つのノード」を用いて「1番目のノードを頂点とする部分木の葉からなる集合 ー
2番目のノードを頂点とする部分木の葉からなる集合」を表す.
Ex) Node i,j == Subset i,j (S_i,j) == {u1,..., u8} ー {u5, u6} = {u1,u2, u3, u4, u7, u8}
i が j の先祖であるようなすべてのノードの組 (i,j) についてこのような集合を定義する.
u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16

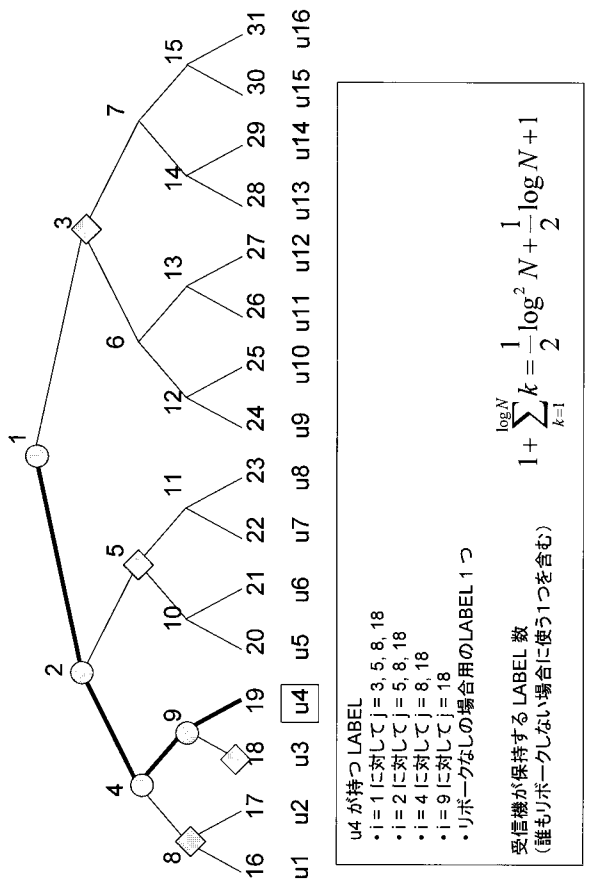
【図７】


(A)
S = LABEL_i
T = G_L(S)
G_L(T)
LC(k)
G_R(T)
RC(k)
G_L(G_R(S))
G_R(S)
G_R(G_R(S))
G_L(G_R(G_L(S)))
(B)
C bit
あるノードの LABEL
G
PRNG（擬似乱数生成器）
LABEL_i,j = G_L(G_R(LABEL_i))
SK_i,j = G_M(LABEL_i,j)
3C bit
G_L(T)
G_M(T)
G_R(T)
左の子の LABEL
そのノードの KEY
右の子の LABEL

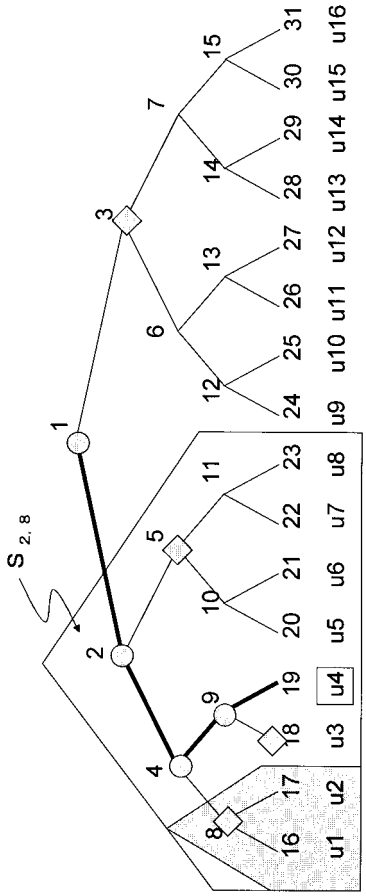
【図８】


(A)
受信機 u は、u からルートへのパス上のある i について、u から i へのパスから枝分かれしているノードの LABEL のみ保持すればよい
(a)
リボーク部
d251
(b)
リボーク部
(c)
リボーク部

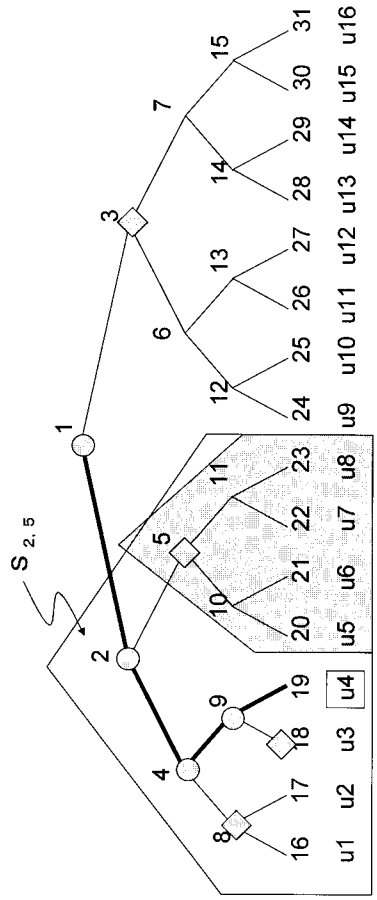
【図９】



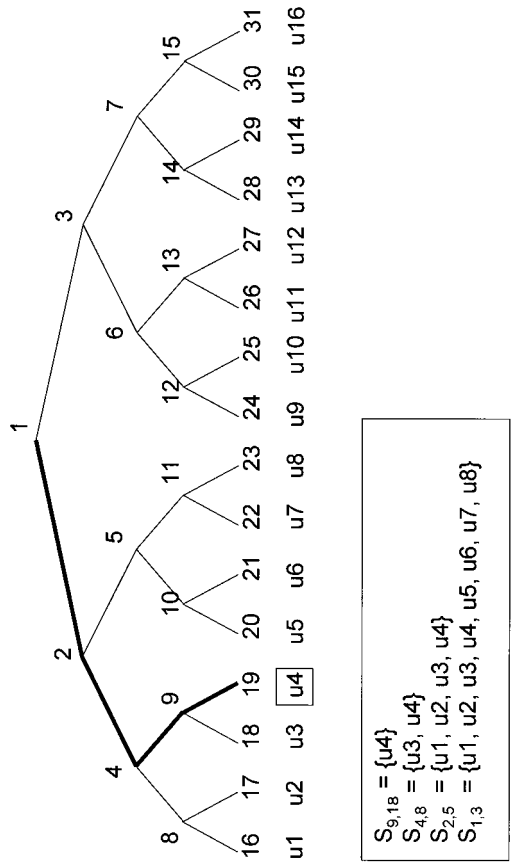

【図１０】



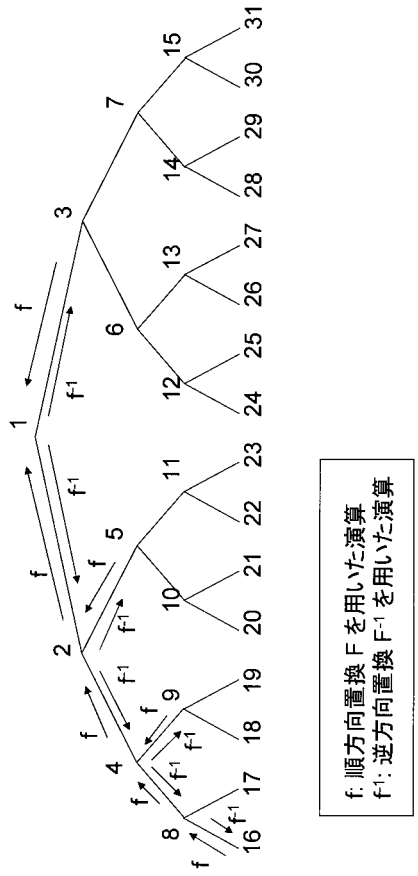

【図１１】



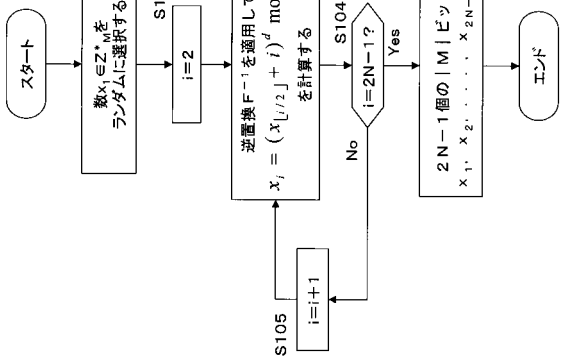

【図１２】



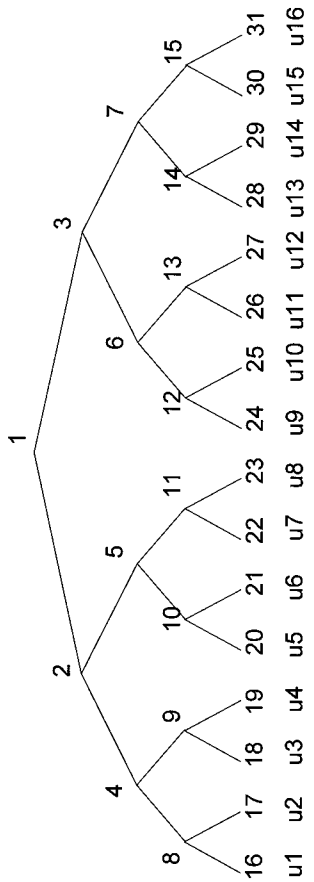
【図１３】



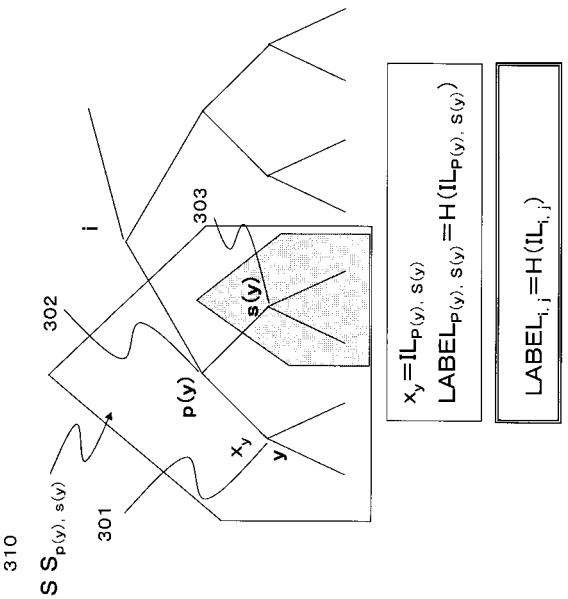

【図１４】



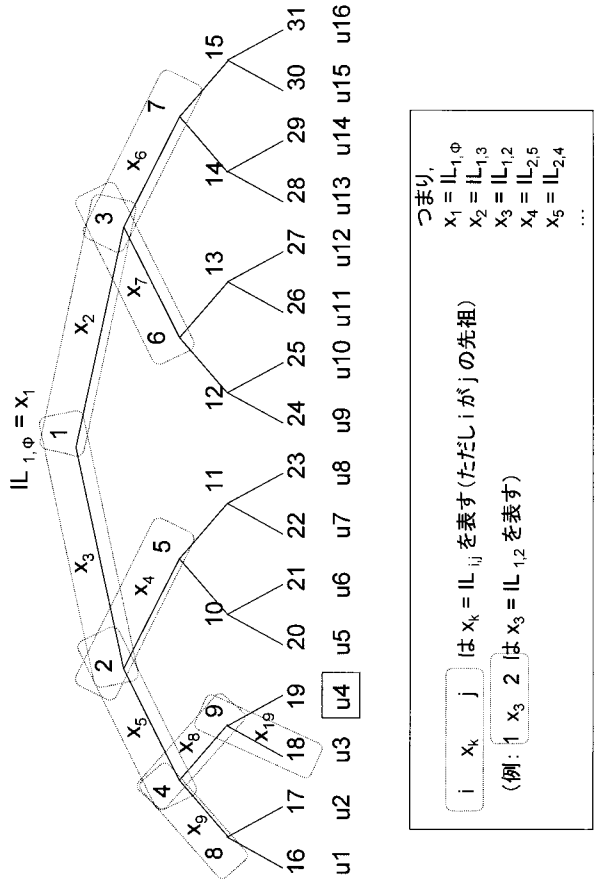

【図１５】



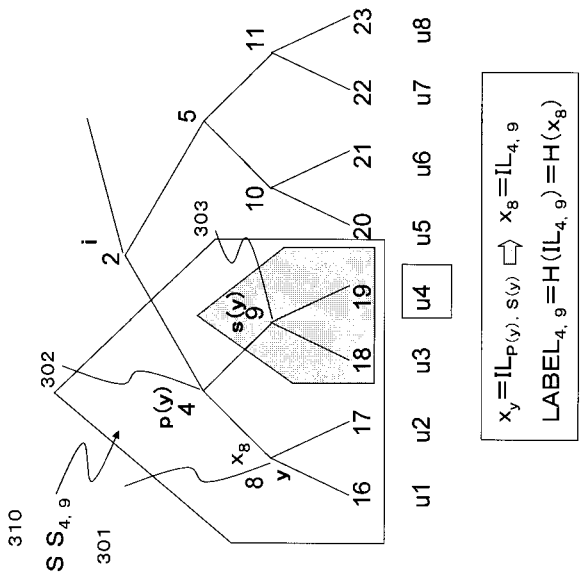

【図１６】



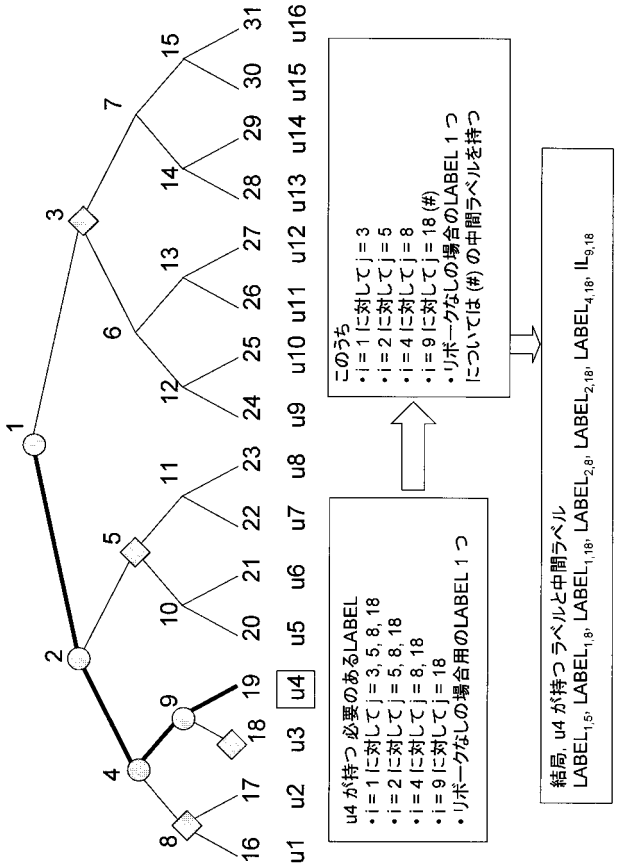
【図１７】



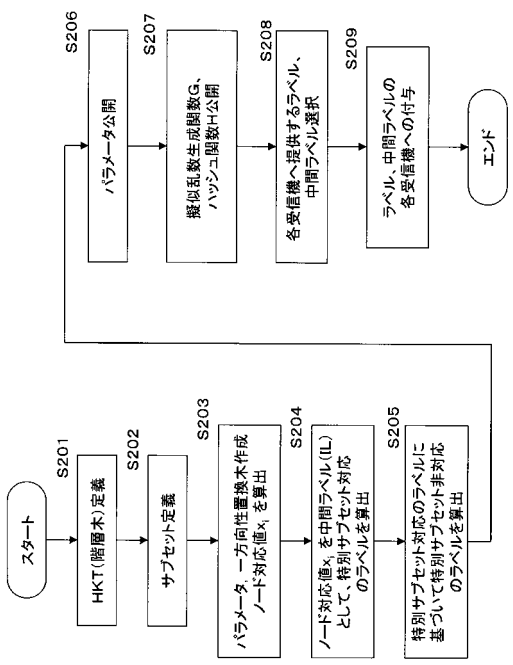

【図１８】



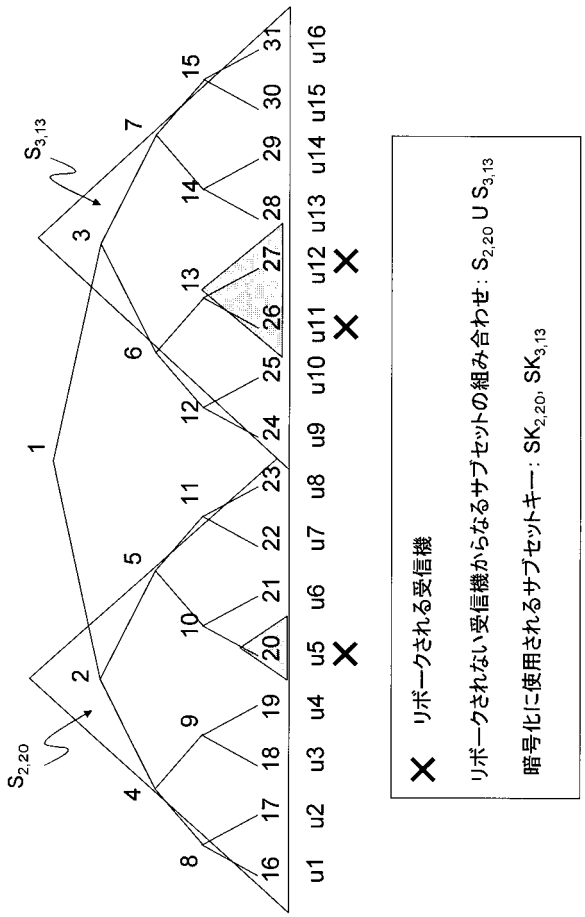

【図１９】



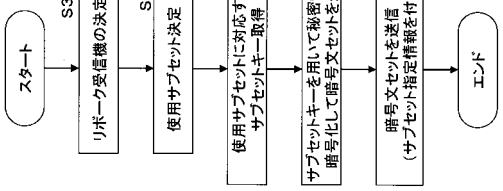

【図２０】



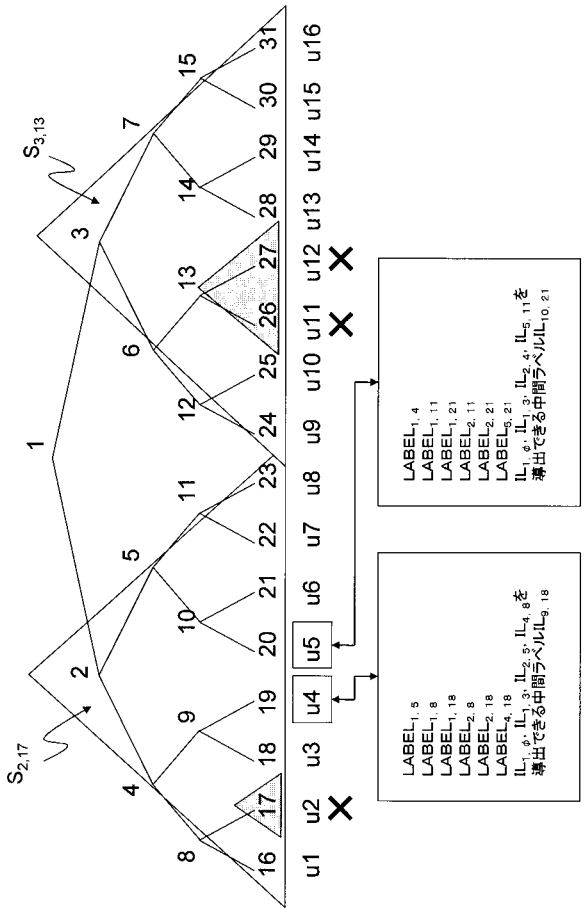
【図２１】



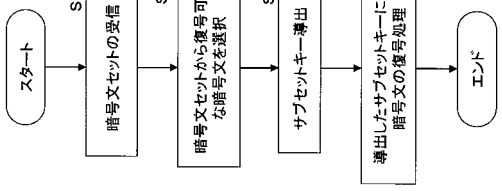

【図２２】



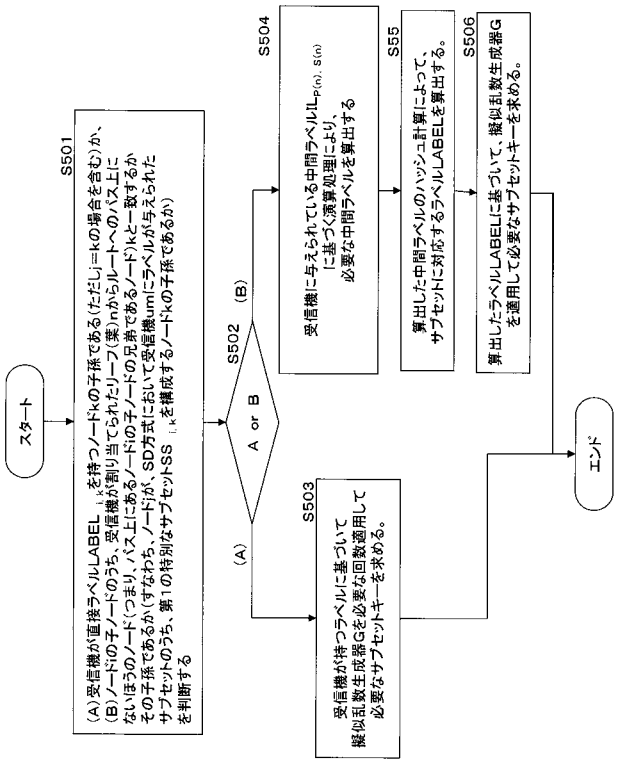

【図２３】



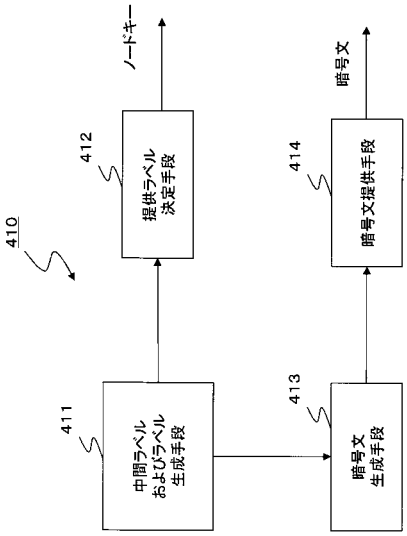

【図２４】



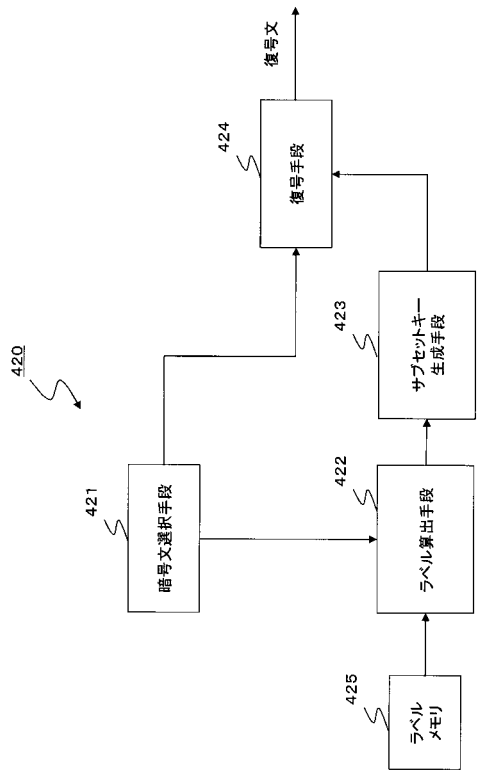
【図２５】



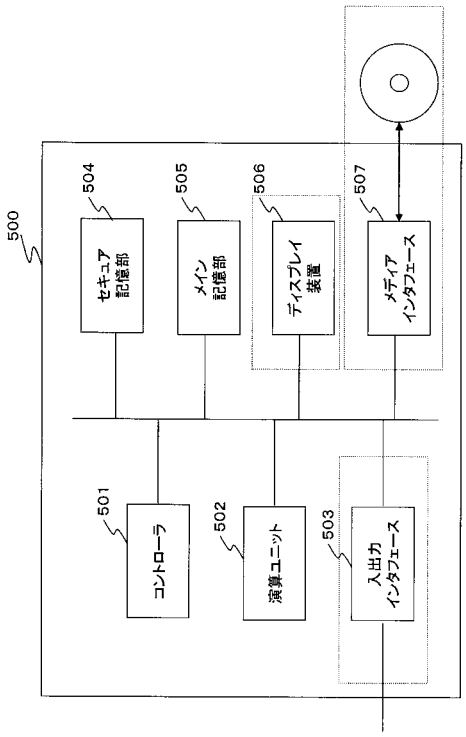

【図２６】



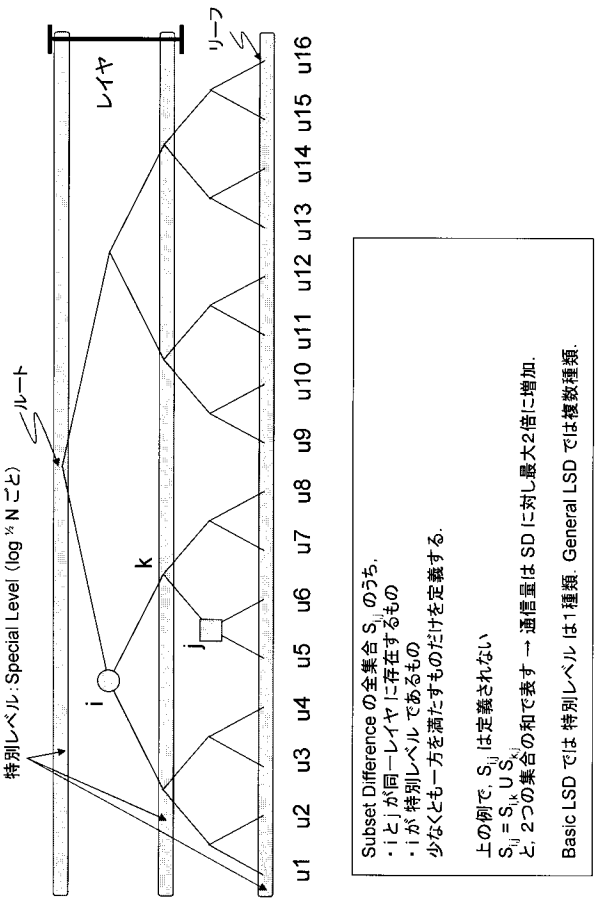

【図２７】



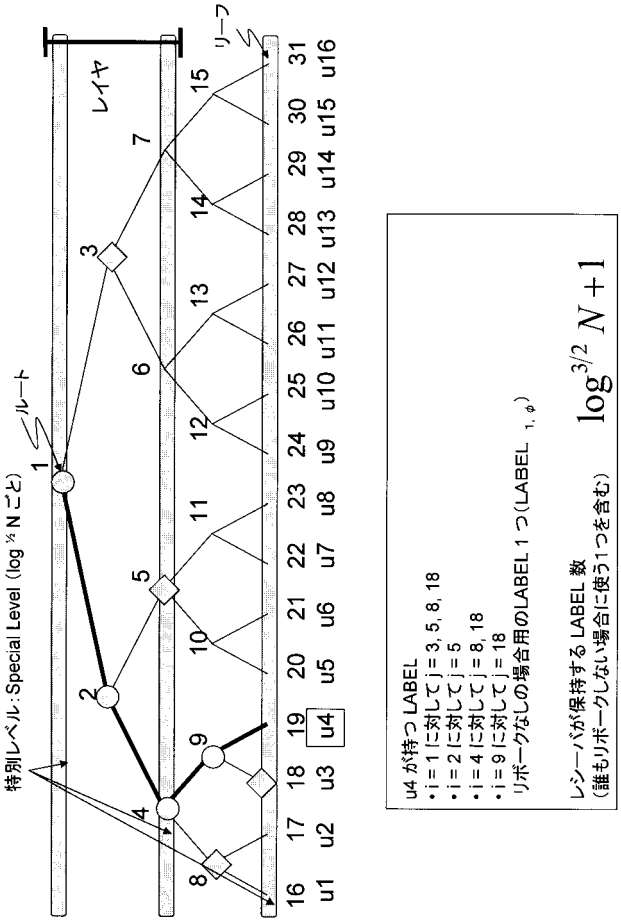

【図２８】



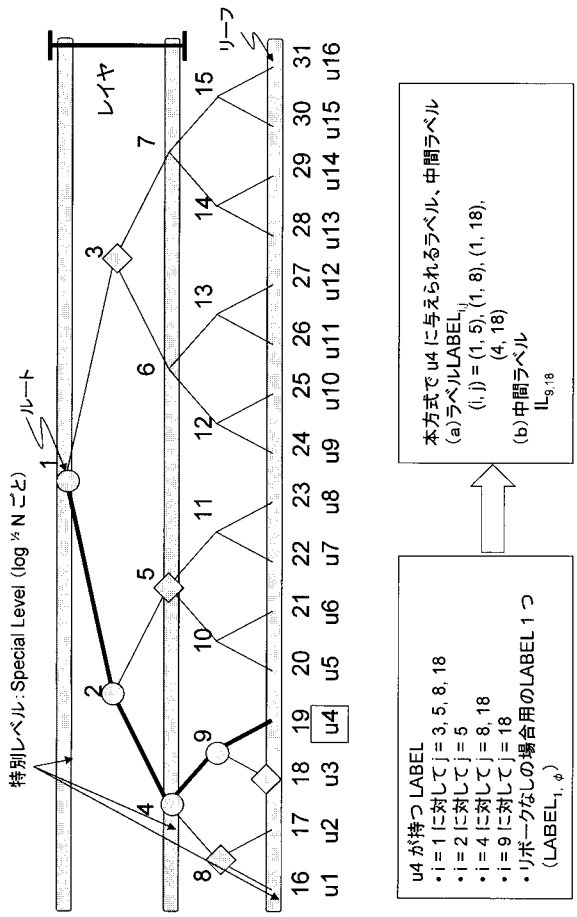
【図２９】


特別レベル：Special Level (log ½ N ごと)
ルート
レイヤ
リーフ
i
j
k
u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16
Subset Difference の全集合 $S_{ij}$ のうち,
・i と j が同一レイヤに存在するもの
・i が 特別レベル であるもの
少なくとも一方を満たすものだけを定義する.
上の例で, $S_{ij}$ は定義されない
$S_{ij} = S_{ik} \cup S_{kj}$
と, 2つの集合の和で表す → 通信量は SD に対し最大2倍に増加.
Basic LSD では 特別レベル は1種類. General LSD では複数種類.

【図３０】


特別レベル：Special Level (log ½ N ごと)
ルート
レイヤ
リーフ
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16
u4 が持つ LABEL
• i = 1 に対して j = 3, 5, 8, 18
• i = 2 に対して j = 5
• i = 4 に対して j = 8, 18
• i = 9 に対して j = 18
リボークなしの場合用のLABEL 1 つ($LABEL_{1,\phi}$)
レシーバが保持する LABEL 数
(誰もリボークしない場合に使う1つを含む)
$\log^{3/2} N + 1$

【図３１】


特別レベル：Special Level (log ½ N ごと)
ルート
レイヤ
リーフ
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16
u4 が持つ LABEL
• i = 1 に対して j = 3, 5, 8, 18
• i = 2 に対して j = 5
• i = 4 に対して j = 8, 18
• i = 9 に対して j = 18
• リボークなしの場合用のLABEL 1 つ
($LABEL_{1,\phi}$)
本方式で u4 に与えられるラベル、中間ラベル
(a)ラベルLABEL$_{i,j}$
(i, j) = (1, 5), (1, 8), (1, 18),
(4, 18)
(b) 中間ラベル
$IL_{9,18}$