(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4635459号
(P4635459)
(45)発行日　平成23年2月23日(2011.2.23)　(24)登録日　平成22年12月3日(2010.12.3)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 18　(全 67 頁)

(21)出願番号　特願2004-73057(P2004-73057)
(22)出願日　平成16年3月15日(2004.3.15)
(65)公開番号　特開2005-260852(P2005-260852A)
(43)公開日　平成17年9月22日(2005.9.22)
審査請求日　平成18年10月30日(2006.10.30)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　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

審査官　新田　亮

最終頁に続く

(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)【特許請求の範囲】
【請求項１】
情報処理装置において、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方法であり、
前記情報処理装置のラベル生成手段が、階層木を適用したＳＤ（Ｓｕｂｓｅｔ　Ｄｉｆｅｒｅｎｃｅ）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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定したラベルを生成するラベル生成ステップと、
前記情報処理装置の提供ラベル決定手段が、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、
前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルと、
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】
情報処理装置において、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、
前記情報処理装置は、
前記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しない特別サブセット非対応ラベルと、
前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを記憶部に保持し、
前記情報処理装置の暗号文選択手段が、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、
前記情報処理装置のラベル算出手段が、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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なるラベルを算出するラベル算出ステップと、
前記情報処理装置のサブセットキー生成手段が、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、
前記情報処理装置の復号手段が、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３】
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、
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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定した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、
前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応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４】
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する暗号文生成手段と、
前記暗号文を前記受信機に提供する暗号文提供手段と、
を有することを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記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３に記載の情報処理装置。
【請求項６】

前記ラベル生成手段は、
階層木において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、選択された特別サブセットに対応するラベルの値を、該特別サブセットの直下に設定される他の特別サブセットの値に対する一方向性関数Ｆの適用によって算出可能としたラベルを生成することを特徴とする請求項３に記載の情報処理装置。
【請求項７】
前記ラベル生成手段は、
末端ノード数Ｎの２分木構成を持つ階層木においてＮ個の値：x_N～x_{2N-1}を決定し、ｉ＝２Ｎ－１とする初期設定を実行し、ｉ＝（２Ｎ－１）～１において、ｉ＝偶数の場合に、一方向性関数Ｆを適用しＦ（x_i）を計算し、これを$x_{i/2}$とセットする構成を有し、上記各処理によって、末端ノード数Ｎの２分木構成において、２Ｎ－１個の特別サブセット対応のラベルの値：x_1～x_{2N-1}を決定する構成であることを特徴とする請求項３に記載の情報処理装置。
【請求項８】
前記提供ラベル決定手段は、
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$SS_{i,j}$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、下記条件、
（ａ）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$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれでもないサブセット対応のラベル$LABEL_{i,j}$と、
（ｂ）仮選択ラベルから、前記第１の特別なサブセット$SS_{i,j}$、および、前記第２の特別なサブセット$SS_{1,\phi}$のいずれかに対応するラベルであり、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
である値ｙに対応する値x_yに対応するラベル$LABEL_{i,j}$と、
上記（ａ）または（ｂ）の条件を満足するラベルを、受信機ｕｍに対する最終提供ラベルとして決定する構成であることを特徴とする請求項３に記載の情報処理装置。
【請求項９】
前記提供ラベル決定手段は、
受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［x_y＝$LABEL_{P(y),S(y)}$］に加えてｊ個のラベル、（ただし、ｊは０以上ｌｏｇＮ、Ｎは、前記階層木における末端ノード数＝受信機数）、
を受信機に対する特別サブセット対応の提供ラベル数とする構成であることを特徴とする請求項３に記載の情報処理装置。
【請求項１０】
前記一方向性関数Ｆは、
ＭＤ４またはＭＤ５またはＳＨＡ－１であることを特徴とする請求項３に記載の情報処理装置。
【請求項１１】
前記ラベル決定手段は、
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の値を、異なる特別サブセット対応のラベル（ＬＡＢＥＬ）値に対する前記一方向関数Ｆの適用により算出可能な値として設定する

構成であることを特徴とする請求項３乃至１０いずれかに記載の情報処理装置。
【請求項１２】
前記ラベル決定手段は、
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値を、異なる特別サブセット対応のラベル（ＬＡＢＥＬ）値に対する前記一方向関数Ｆの適用により算出可能な値として設定する構成であることを特徴とする請求項３乃至１０いずれかに記載の情報処理装置。
【請求項１３】
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しない特別サブセット非対応ラベルと、
前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを格納した記憶部と、
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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なる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１４】
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、保持している他のラベルに対する一方向性関数Ｆの適用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１３に記載の情報処理装置。
【請求項１５】
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一方向性関数を適用して実行する構成であることを特徴とする請求項１４に記載の情報処理装置。
【請求項１６】
前記一方向性関数Ｆは、
ＭＤ４またはＭＤ５またはＳＨＡ－１であることを特徴とする請求項１３に記載の情報処理装置。
【請求項１７】

情報処理装置において、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させるコンピュータ・プログラムであり、
前記情報処理装置のラベル生成手段に、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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定したラベルを生成させるラベル生成ステップと、
前記情報処理装置の提供ラベル決定手段に、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させるステップであり、
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、
前記特別サブセットに対応するラベルであって、受信機に提供されるラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルと、
を受信機に対する提供ラベルとして決定させ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１８】
情報処理装置において、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させるコンピュータ・プログラムであり、
前記情報処理装置は、
前記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しない特別サブセット非対応ラベルと、
前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを記憶部に保持し、
前記情報処理装置の暗号文選択手段に、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させる暗号文選択ステップと、
前記情報処理装置のラベル算出手段に、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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なるラベルを算出させるラベル算出ステップと、
前記情報処理装置のサブセットキー生成手段に、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させるステップと、
前記情報処理装置の復号手段に、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させる復号ステップと、
を有することを特徴とするコンピュータ・プログラム。
【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　Ｔｒａｃｉｎｇ　Ｓｃｈｅｍｅｓ　ｆｏｒ　Ｓｔａｔｅｌｅｓｓ　Ｒｅｃｅｉｖｅｒｓ"」

【非特許文献２】Ａｄｖａｎｃｅｓ　ｉｎ　Ｃｒｙｐｔｏｇｒａｐｈｙ－Ｃｒｙｐｔｏ２００２，　Ｌｅｃｔｕｒｅ　Ｎｏｔｅｓ　ｉｎ　Ｃｏｍｐｕｔｅｒ　Ｓｃｉｅｎｃｅ２４４２，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一方向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、

情報処理装置において、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方法であり、

前記情報処理装置のラベル生成手段が、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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定したラベルを生成するラベル生成ステップと、

前記情報処理装置の提供ラベル決定手段が、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、

前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルと、

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。

【００３１】

さらに、本発明の第２の側面は、

情報処理装置において、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、

前記情報処理装置は、

前記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しない特別サブセット非対応ラベルと、

前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを記憶部に保持し、

前記情報処理装置の暗号文選択手段が、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、

前記情報処理装置のラベル算出手段が、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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なるラベルを算出するラベル算出ステップと、

前記情報処理装置のサブセットキー生成手段が、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、

前記情報処理装置の復号手段が、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。

【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、

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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定した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、

前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応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。

【００３６】

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する暗号文生成手段と、前記暗号文を前記受信機に提供する暗号文提供手段とを有することを特徴とする。

【００３７】

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。

【００３８】
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、階層木において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、選択された特別サブセットに対応するラベルの値を、該特別サブセットの直下に設定される他の特別サブセットの値に対する一方向性関数Ｆの適用によって算出可能としたラベルを生成することを特徴とする。
【００３９】
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、末端ノード数Ｎの２分木構成を持つ階層木においてＮ個の値：x_N～x_{2N-1}を決定し、ｉ＝２Ｎ－１とする初期設定を実行し、ｉ＝（２Ｎ－１）～１において、ｉ＝偶数の場合に、一方向性関数Ｆを適用しＦ（x_i）を計算し、これを$x_{i/2}$とセットする構成を有し、上記各処理によって、末端ノード数Ｎの２分木構成において、２Ｎ－１個の特別サブセット対応のラベルの値：x_1～x_{2N-1}を決定する構成であることを特徴とする。
【００４０】
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、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、下記条件、
（ａ）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$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれでもないサブセット対応のラベル$LABEL_{i,j}$と、
（ｂ）仮選択ラベルから、前記第１の特別なサブセット$SS_{i,j}$、および、前記第２の特別なサブセット$SS_{1,\phi}$のいずれかに対応するラベルであり、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
である値ｙに対応する値x_yに対応するラベル$LABEL_{i,j}$と、
上記（ａ）または（ｂ）の条件を満足するラベルを、受信機ｕｍに対する最終提供ラベルとして決定する構成であることを特徴とする。
【００４１】
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、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［x_y＝$LABEL_{P(y),S(y)}$］に加えてｊ個のラベル、（ただし、ｊは０以上ｌｏｇＮ、Ｎは、前記階層木における末端ノード数＝受信機数）、を受信機に対する特別サブセット対応の提供ラベル数とする構成であることを特徴とする。
【００４２】
さらに、本発明の情報処理装置の一実施態様において、前記一方向性関数Ｆは、ＭＤ４またはＭＤ５またはＳＨＡ－１であ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、前記ラベル決定手段は、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の値を、異なる特別サブセット対応のラベル（ＬＡＢＥＬ）値に対する前記一方向関数Ｆの適用により算出可能な値として設定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、前記ラベル決定手段は、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値を、異なる特別サブセット対応のラベル（ＬＡＢＥＬ）値に対する前記一方向関数Ｆの適用により算出可能な値として設定する構成であることを特徴とする。

【００４５】

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しない特別サブセット非対応ラベルと、

前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを格納した記憶部と、

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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なる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。

【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、保持している他のラベルに対する一方向性関数Ｆの適用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。

【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一方向性関数を適用して実行する構成であ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、前記一方向性関数Ｆは、ＭＤ４またはＭＤ５またはＳＨＡ－１であることを特徴とする。

【００４９】

さらに、本発明の第５の側面は、

情報処理装置において、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させるコンピュータ・プログラムであり、

前記情報処理装置のラベル生成手段に、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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定したラベルを生成させるラベル生成ステップと、

前記情報処理装置の提供ラベル決定手段に、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させるステップであり、

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、

前記特別サブセットに対応するラベルであって、受信機に提供されるラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルと、

を受信機に対する提供ラベルとして決定させ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。

【００５１】

さらに、本発明の第６の側面は、

情報処理装置において、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させるコンピュータ・プログラムであり、

前記情報処理装置は、

前記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しない特別サブセット非対応ラベルと、

前記特別サブセットに対応するラベルであって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを記憶部に保持し、

前記情報処理装置の暗号文選択手段に、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させる暗号文選択ステップと、

前記情報処理装置のラベル算出手段に、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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なるラベルを算出させるラベル算出ステップと、

前記情報処理装置のサブセットキー生成手段に、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させるステップと、

前記情報処理装置の復号手段に、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させる復号ステップと、

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。

【００５２】

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。

【００５３】

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】

【００５４】
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、さらに一方向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。
【００５５】
さらに、本発明の構成によれば、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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定し、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であって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを受信機に対する提供ラベルとしたので、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、受信機側の保持ラベルに対する一方向性関数Ｆの適用により算出可能であり、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】
【００５６】
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。
【００５７】
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
３．一方向木を用いたＳＤ方式のラベル数削減構成
４．一方向木の構成方法例
５．一方向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
９．一方向木を用いた一般化ＬＳＤ方式のラベル数削減構成
【００５８】
［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。
【００５９】
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。

【００６０】

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

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）

ＬＣ（ｉ）：ノードｉの左側の子ノード

ＲＣ（ｉ）：ノードｉの右側の子ノード

【００６１】

（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。

【００６２】

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。

【００６３】

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。

【００６４】

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。

【００６５】

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。

【００６６】

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。

【００６７】

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。

【００６８】

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。

【００６９】

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。

【００７０】

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。

【００７１】

［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。

【００７２】

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。

【００７３】

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。

【００７４】

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１】

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

【００７５】
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。
【００７６】
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。
【００７７】
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。
【００７８】
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。
【００７９】
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$LABEL_{i,RC(k)}$
【００８０】
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。
【００８１】

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。

【００８２】

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。

【００８３】

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。

【００８４】

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。

【００８５】

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。

【００８６】

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。

【００８７】

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。

【００８８】

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。

【００８９】

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。

【００９０】

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。

【００９１】

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。

【００９２】

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。

【００９３】

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。

【００９４】

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$Ｓ_{１，\phi}$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。

【００９５】

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。

【００９６】

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。

【００９７】

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２】

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

【００９８】

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。

【００９９】

［３．一方向木を用いた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。

【０１００】

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。

【０１０１】

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。

【０１０２】

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。

【０１０３】
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。
【０１０４】
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。
【０１０５】
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。
【０１０６】
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。
【０１０７】
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、一方向性関数を適用した鍵の木構造、すなわち一方向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。
【０１０８】
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個保持しており、上記の工夫によりそのうちいくつかを１つの値から一方向性関数などを適用して導出可能な設定とすることにより、受信機の保持すべきラベル数を削減する。
【０１０９】
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、以下において説明する一方向木を適用することで、受信機の保持すべきラベル数を削減することが可能となる。

【０１１０】

［４．一方向木の構成例］

以下、本発明にかかる一方向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。

【０１１１】

「一方向木」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それぞれＣビット（たとえば１２８ビット）の値x_i（ｉ＝１，２，...，２Ｎ－１）を設定し、ｉ＝１，２，...，Ｎ－１について、$x_i = F(x_{2i})$が成り立つ木構造をいうものとする。

【０１１２】

ここで、関数Ｆは、Ｃビットの入力に対して、Ｃビットの出力を出す一方向性関数である。

【０１１３】

このような関数の例として、任意の長さの入力に対し１２８ビットの出力を出すＭＤ４，ＭＤ５や、１６０ビットの出力を出すＳＨＡ－１などがあり、これらの関数を適用することができる。なお、これらの関数については、たとえば、Ａ．Ｊ．Ｍｅｎｅｚｅｓ，Ｐ．Ｃ．ｖａｎ Ｏｏｒｓｃｈｏｔ ａｎｄ Ｓ．Ａ．Ｖａｎｓｔｏｎｅ著，"Ｈａｎｄｂｏｏｋ ｏｆＡｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ"，ＣＲＣ Ｐｒｅｓ，１９９６に紹介されている。なお、これらの関数は一方向性関数、あるいはハッシュ関数と呼ばれる。

【０１１４】

一方向木を構成する各ノードｉに対応して設定される関数Ｆとノード対応値x_iの関係を図で表すと、図１３のようになる。この一方向木を構成する木構造は、上位ノードと下位ノードのノード対応値x_iについて、$x_i = F(x_{2i})$が成り立つ木構造である。

例えば、
$x_8 = F(x_{16})$
$x_4 = F(x_8)$
$x_2 = F(x_4)$
$x_1 = F(x_2)$
のように、２分木の構成ノードｉに対応して設定されるノード対応値x_iは、$x_i = F(x_{2i})$が成り立つように設定される。

【０１１５】

葉（リーフ）がＮ個である２分木において、一方向木を構成するアルゴリズムの例を下

記に示す。このアルゴリズムにおいて、入力と出力は、以下のように設定される。
［入力］
２分木を構成する葉（リーフ）の数Ｎ、
Ｃビット出力の一方向性関数Ｆ、
［出力］
２分木を構成する全ノード（葉（リーフ）を含む）数：２Ｎ－１に対応する２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}
である。
【０１１６】
上記の［入力］に基づいて、上記の［出力］を得るアルゴリズムは以下のようになる。
１．Ｎ個のＣビットの数x_N，x_{N+1}，...，x_{2N-1}を独立に選択する。
２．ｉをカウンタとして２Ｎ－１から１まで１ずつ減少させながら下記の処理を行う。
（２－１）もしｉが偶数なら、関数Ｆを適用しＦ（x_i）を計算し、これを$x_{i/2}$とセットする。
３．２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}を出力して終了する。値x_iが一方向木のノード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。
【０１１７】
図１４に、上記アルゴリズムのフローを示す。フローの各ステップについて説明する。ステップＳ１０１において、２分木を構成する葉（リーフ）の数Ｎと、Ｃビット出力の一方向性関数Ｆを入力する。
【０１１８】
ステップＳ１０２において、Ｎ個のＣビットの数x_N，x_{N+1}，...，x_{2N-1}を独立に選択する。ステップＳ１０３において、値：ｉの初期設定として、ｉ＝２Ｎ－１とする設定を行なう。
【０１１９】
ステップＳ１０４において、ｉは偶数か否かを判定する。ｉが偶数の場合はステップＳ１０５に進み、ｉが奇数の場合はステップＳ１０６に進む。
【０１２０】
ｉが偶数の場合は、ステップＳ１０５において、関数Ｆを適用しＦ（x_i）を計算し、これを$x_{i/2}$とセットする。
【０１２１】
ステップＳ１０６では、ｉ＝１であるか否かを判定し、ｉ＝１でない場合は、ステップＳ１０７に進み、値ｉをｉ＝ｉ－１とする更新処理を実行し、ステップＳ１０４以下の処理を繰り返し実行する。
【０１２２】
ステップＳ１０６でｉ＝１であると判定すると、ステップＳ１０８に進み、２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}を各ノードｉに対応するノード対応値x_iとして出力する。
【０１２３】
この２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}が、２Ｎ－１個のノード（リーフを含む）の各ノードｉ（ｉ＝１～２Ｎ－１）各々に対応する値として設定される。
【０１２４】
この処理によって、一方向木を構成する各ノードｉに対応するノード対応値x_iが決定され、一方向木構造が完成する。
【０１２５】
なお、上述の一方向木の設定処理例では、図１３に示すように、下位ノードから右上がりの上位ノードを一方向性関数Ｆを適用して算出可能な構成としたが、下位ノードから左上がりの上位ノードを一方向性関数Ｆを適用して算出可能な構成としてもよい。

【０１２６】
［５．一方向木を適用した情報配信処理例］
次に、上述した一方向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。
【０１２７】
（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。
【０１２８】
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。
【０１２９】
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。
【０１３０】
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。
【０１３１】
さらに、管理センタ（ＴＣ）は、Ｃビット出力の一方向関数Ｆを選択して公開する。Ｃは任意の数であり、一方向性関数は、例えばＭＤ４、ＭＤ５、ＳＨＡ－１など既存の一方向性関数（ハッシュ関数）の適用が可能である。
【０１３２】
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。
【０１３３】
ｂ．ステップ２
管理センタ（ＴＣ）は、先に図８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分木における各ノードｉの対応値x_iを算出する。すなわち、
（ａ）２分木を構成する葉（リーフ）の数Ｎ、
（ｂ）Ｃビット出力の一方向性関数Ｆ、
を入力として、２分木を構成する全ノード（葉（リーフ）を含む）数：２Ｎ－１に対応

する２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}
を決定する。
【０１３４】
管理センタ（ＴＣ）は、図１４を参照して説明したアルゴリズム、すなわち、
［入力］
２分木を構成する葉（リーフ）の数Ｎ、
Ｃビット出力の一方向性関数Ｆ、
［出力］
２分木を構成する全ノード（葉（リーフ）を含む）数：２Ｎ－１に対応する２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}
に従って２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}を定める。
【０１３５】
管理センタ（ＴＣ）は、上記２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}中の値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$SS_{1,\phi}$のラベルとする。すなわち、
$LABEL_{1,\phi}=x_1$
とする。
【０１３６】
また、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$LABEL_{i,j}$を下記のように定める。すなわち、前述の処理によってノード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$SS_{P(y),S(y)}$に対応するラベル$LABEL_{P(y),S(y)}$とする。すなわち、
$x_y=LABEL_{P(y),S(y)}$
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。
【０１３７】
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算出される値であり、
$F(x_i)=x_{i/2}$
を満足する。
【０１３８】
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、すなわち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$SS_{P(y),S(y)}$は、図１６に示すサブセット$SS_{P(y),S(y)}$３１０である。
【０１３９】
このとき、サブセット$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、ノードｙ３０１に対応するノード対応値としてのx_yとする。すなわち、
$x_y=LABEL_{P(y),S(y)}$
とする。
【０１４０】
上記処理をまとめると、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Ｃビットの数x_1，x_2，...，x_{2N-1}中の１つの値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$SS_{1,\phi}$のラベルとし、その他のx_2，...，x_{2N-1}の値を、、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$LABEL_{i,j}$として設定する。すなわち、

$LABEL_{1,\phi}=x_1$

と設定し、

さらに、ｙ＝１，２，...，Ｎ－１に対して、

$LABEL_{y,2y}=x_{2y+1}$

$LABEL_{y,2y+1}=x_{2y}$

とする。

【０１４１】

図１７（１）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Ｃビットの数x_1，x_2，...，x_{2N-1}との対応を示す。

【０１４２】

図１７（２）に示すように、２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}のそれぞれは、下記のように、各ラベルの値として設定される。

$x_1=LABEL_{1,\Phi}$

$x_2=LABEL_{1,3}$

$x_3=LABEL_{1,2}$

$x_4=LABEL_{2,5}$

$x_5=LABEL_{2,4}$

：　　：

$x_{30}=LABEL_{15,31}$

$x_{31}=LABEL_{15,30}$

【０１４３】

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、

の各ラベルの値を、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Ｃビットの数x_1，x_2，...，x_{2N-1}に対応付けて決定する。

【０１４４】

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。

【０１４５】

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。

【０１４６】

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。

【０１４７】

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。

【０１４８】

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。

【０１４９】

図１８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１８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。

【０１５０】

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。

【０１５１】

これらの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。

【０１５２】

管理センタ（ＴＣ）は、階層木の末端ノードとしての葉（リーフ）に対応して設定される受信機ｕｍ（ｍ＝１，２，...，Ｎ）に対し、以下のルールに基づいて、提供ラベルを決定する。

【０１５３】

例えば、図１９に示すような階層木において、受信機はノード番号ｙ＝１６～３１にそれぞれｕ１からｕ１６まで割り当てられ、計１６個設定される。

【０１５４】

受信機ｕｍが割り当てられた葉からルートへのパスをパスｍ［ｐａｔｈ－ｍ］と表す。また、パスｍ［ｐａｔｈ－ｍ］上のノードｙの集合をパスノードｍ［ＰａｔｈＮｏｄｅｓ－ｍ］と表す。

【０１５５】

図１９の例では、
ＰａｔｈＮｏｄｅｓ－１＝｛１，２，４，８，１６｝
ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝
ＰａｔｈＮｏｄｅｓ－１１＝｛１，３，６，１３，２６｝
となる。

【０１５６】

図１９に示す実線ライン３２１が、受信機ｕ１のパス１［ｐａｔｈ－１］３２１であり、ＰａｔｈＮｏｄｅｓ－１＝｛１，２，４，８，１６｝によって構成される。点線ライン３２２が、受信機ｕ４のパス４［ｐａｔｈ－４］３２２であり、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝によって構成される。破線ライン３２３が、受信機ｕ１１のパス１１［ｐａｔｈ－１１］３２３であり、ＰａｔｈＮｏｄｅｓ－１１＝｛１，３，６，１３，２６｝によって構成される。

【０１５７】

管理センタ（ＴＣ）は、図１８を参照して説明した仮選択ラベルのうち以下の条件（ａ）を満足するラベルと、以下の条件（ｂ）を満足するラベルをそれぞれ選択して、各受信機ｕｍに対する最終的な提供ラベルを決定する。

【０１５８】

（ａ）仮選択ラベル中、いずれの特別なサブセットにも該当しないもの、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$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれでもないサブセット対応のラベル$LABEL_{i,j}$。

（ｂ）仮選択ラベル中、いずれか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$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれかに対応するラベルであり、

（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、

（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード

である値ｙに対応する値x_yに対応するラベル$LABEL_{i,j}$。

上記（ａ）の条件を満足するラベルと、（ｂ）の条件を満足するラベルとが、受信機ｕｍに提供される。

【０１５９】

具体的な例を、図２０を参照して説明する。図２０に示す階層木中、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、まず、

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

【０１６０】

この中から、まず、上記条件（ａ）を満足するラベル、すなわち、第１および第２の特別なサブセットのいずれにも対応しないラベルを選択する。これは、第１の特別なサブセット$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれにも対応しないサブセット対応のラベルである。すなわち、

$LABEL_{1,5}$、$LABEL_{1,8}$、$LABEL_{1,18}$、$LABEL_{2,8}$、$LABEL_{2,18}$、$LABEL_{4,18}$の６個のラベルが選択されて受信機ｕ４に与えられる。

【０１６１】

さらに、上記条件（ｂ）を満足するラベルを仮選択ラベルから選択する。すなわち、第１または第２の特別なサブセットのいずれかに対応するラベルであり、

（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、

（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード

として選択されるノード番号ｙに対応して設定される値x_yに対応するラベルＬＡＢＥＬ$_{i,j}$。

【０１６２】

ノード番号ｙと、２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}のそれぞれは、先に図１６（１）を参照して説明したような関係にあり、さらに、２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}のそれぞれは、図１６（２）に示すように、各ラベルの値として設定されている。すなわち、

x_1＝ＬＡＢＥＬ$_{1,\Phi}$

x_2＝ＬＡＢＥＬ$_{1,3}$

x_3＝ＬＡＢＥＬ$_{1,2}$

x_4＝ＬＡＢＥＬ$_{2,5}$

x_5＝ＬＡＢＥＬ$_{2,4}$

：　　：

x_{30}＝ＬＡＢＥＬ$_{15,31}$

x_{31}＝ＬＡＢＥＬ$_{15,30}$

である。

【０１６３】

図２０に示す階層木中、ノード番号１９に対応する受信機ｕ４のパス－ｍは、図１９に示すパス４［ｐａｔｈ－４］３２２であり、パス４［ｐａｔｈ－４］３２２に含まれるノードとしてのパスノード４は、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝となる。

ここで、

（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、

（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード

を満足するノード番号ｙを選択する。

【０１６４】

受信機ｕ４において、

（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれ、

の条件を満足するノードは、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝の各ノードである。

この中で、

（ｂ２）ノード２ｙが含まれていないノード

は、ノード４，９，１９となる。ノード１，２については、

ノード１は、ノード２×１に対応するノード２が、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝中に含まれ、また、

ノード２は、ノード２×２に対応するノード４が、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝中に含まれる。

【０１６５】

従って、受信機ｕ４において、

（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれ、かつ、

（ｂ２）ノード２ｙが含まれていないノード

これらの条件（ｂ１），（ｂ２）を満足するノードは、ノード番号はｙ＝４，９，１９となる。

【０１６６】

この結果、ｙ＝４，９，１９に対応するノード対応値x_4，x_9，x_{19}に対応するラベル、すなわち、

x_4＝ＬＡＢＥＬ$_{2,5}$

x_9＝ＬＡＢＥＬ$_{4,8}$

x_{19}＝ＬＡＢＥＬ$_{9,18}$

が、条件（ｂ）を満足するラベルとして選択され、受信機ｕ４に対する提供ラベルとして決定される。

【０１６７】

結果として、受信機ｕ４には、

条件（ａ）を満足するラベルとして、

$LABEL_{1,5}$、$LABEL_{1,8}$、$LABEL_{1,18}$、$LABEL_{2,8}$、$LABEL_{2,18}$、$LABEL_{4,18}$の６個のラベル、

条件（ｂ）を満足するラベルとして、

$x_4 = LABEL_{2,5}$、$x_9 = LABEL_{4,8}$、$x_{19} = LABEL_{9,18}$の３個のラベル、

計９個のラベルが提供されるラベルとなる。

【０１６８】

従来の、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$LABEL_{1,\phi}$であり、これは、図１８を参照して説明した受信機ｕ４に対する仮選択ラベルに相当し、

$LABEL_{1,3}$、$LABEL_{1,5}$、$LABEL_{1,8}$、$LABEL_{1,18}$、$LABEL_{2,5}$、$LABEL_{2,8}$、$LABEL_{2,18}$、$LABEL_{4,8}$、$LABEL_{4,18}$、$LABEL_{9,18}$、$LABEL_{1,\phi}$の１１個のラベルが提供されることになるが、本発明の方式においては、上述したように、受信機ｕ４には、９個のラベル、すなわち、

条件（ａ）を満足するラベルとして、

$LABEL_{1,5}$、$LABEL_{1,8}$、$LABEL_{1,18}$、$LABEL_{2,8}$、$LABEL_{2,18}$、$LABEL_{4,18}$の６個のラベル、

条件（ｂ）を満足するラベルとして、

$x_4 = LABEL_{2,5}$、$x_9 = LABEL_{4,8}$、$x_{19} = LABEL_{9,18}$の３個のラベル、

のみが提供されることになる。

【０１６９】

本発明の方式において、受信機ｕ４に付与されない２つのラベルは、

$LABEL_{1,3}$、

$LABEL_{1,\phi}$、

の２つのラベルであるが、

これらのラベルについては、受信機ｕ４は、提供されたラベルから算出する。すなわち、

$LABEL_{1,3} = x_2$

$LABEL_{1,\phi} = x_1$

であり、

受信機ｕ４は、$x_4 = LABEL_{2,5}$を有しており、

前述したノード対応値としての２Ｎ－１個のＣビットの数$x_1, x_2, \ldots, x_{2N-1}$のそれぞれは、前述の図１４のフローを参照して説明したアルゴリズムに従って算出される値であり、

$F(x_i) = x_{i/2}$

を満足する。

【０１７０】

従って、受信機ｕ４は、所有するラベル$x_4 = LABEL_{2,5}$に基づいて、

$F(x_4) = x_2 = LABEL_{1,3}$

$F(x_2) = x_1 = LABEL_{1,\phi}$

を算出することができる。
これらの処理の詳細については、さらに後段で説明する。
【０１７１】
同様に、図２０に示す階層木中、ノード番号１６に対応する受信機ｕ１に対する提供ラベルは、以下のようになる。
まず、仮選択ラベルとして、
$LABEL_{1,3}$、$LABEL_{1,5}$、$LABEL_{1,9}$、$LABEL_{1,17}$、$LABEL_{2,5}$、$LABEL_{2,9}$、$LABEL_{2,17}$、$LABEL_{4,9}$、$LABEL_{4,17}$、$LABEL_{8,17}$、$LABEL_{1,\phi}$の１１個のラベルが選択される。
【０１７２】
この中から、まず、上記条件（ａ）を満足するラベル、すなわち、第１および第２の特別なサブセットのいずれにも対応しないラベルを選択する。これは、第１の特別なサブセット$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれにも対応しないサブセット対応のラベルである。すなわち、
$LABEL_{1,5}$、$LABEL_{1,9}$、$LABEL_{1,17}$、$LABEL_{2,9}$、$LABEL_{2,17}$、$LABEL_{4,17}$の６個のラベルが選択される。
【０１７３】
さらに、上記条件（ｂ）を満足するラベルを仮選択ラベルから選択する。すなわち、第１または第２の特別なサブセットのいずれかに対応するラベルであり、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
として選択されるノード番号ｙに対応して設定される値x_yに対応するラベル$LABEL_{i,j}$である。
【０１７４】
ノード番号１６に対応する受信機ｕ１のパス－ｍは、図１９に示すパス１［ｐａｔｈ－４］３２１であり、パス１［ｐａｔｈ－１］３２１に含まれるノードとしてのパスノード４は、ＰａｔｈＮｏｄｅｓ－１＝｛１，２，４，８，１６｝となる。
ここで、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
を満足するノード番号ｙはｙ＝１６のみである。
【０１７５】
従って、ｙ＝１６に対応するノード対応値x_{16}に対応するラベル、すなわち、
$x_{16}=LABEL_{8,17}$
が、条件（ｂ）を満足するラベルとして選択され、受信機ｕ１に対する提供ラベルとして決定される。
【０１７６】
結果として、受信機ｕ１には、
条件（ａ）を満足するラベルとして、
$LABEL_{1,5}$、$LABEL_{1,9}$、$LABEL_{1,17}$、$LABEL_{2,9}$、$LABEL_{2,17}$、$LABEL_{4,17}$の６個のラベル、
条件（ｂ）を満足するラベルとして、
$x_{16}=LABEL_{8,17}$の１個のラベル、
計７個のラベルが提供されるラベルとなる。
【０１７７】
従来の、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$LABEL_{1,\phi}$であり、これは、図１８を参照して説明した受信機ｕ１に対する仮選択ラベルに相当し、

$LABEL_{1,3}$、$LABEL_{1,5}$、$LABEL_{1,9}$、$LABEL_{1,17}$、$LABEL_{2,5}$、$LABEL_{2,9}$、$LABEL_{2,17}$、$LABEL_{4,9}$、$LABEL_{4,17}$、$LABEL_{8,17}$、$LABEL_{1,\phi}$の１１個のラベルが提供されることになるが、本発明の方式においては、上述したように、受信機ｕ１には、７個のラベルのみが提供されることになる。

【０１７８】

本発明の方式において、受信機ｕ１に付与されない４つのラベルは、

$LABEL_{4,9}$、

$LABEL_{2,5}$、

$LABEL_{1,3}$、

$LABEL_{1,\phi}$、

の４つのラベルであるが、

これらのラベルについては、受信機ｕ１は、提供されたラベルから算出する。すなわち、

$LABEL_{4,9}=x_8$、

$LABEL_{2,5}=x_4$、

$LABEL_{1,3}=x_2$

$LABEL_{1,\phi}=x_1$

であり、

受信機ｕ１は、$x_{16}=LABEL_{8,17}$を有しており、

前述したノード対応値としての２Ｎ－１個のＣビットの数$x_1, x_2, \ldots, x_{2N-1}$のそれぞれは、前述の図１４のフローを参照して説明したアルゴリズムに従って算出される値であり、

$F(x_i)=x_{i/2}$

を満足する。

【０１７９】

従って、受信機ｕ１は、所有するラベル$x_{16}=LABEL_{8,17}$に基づいて、

$F(x_{16})=x_8=LABEL_{4,9}$

$F(x_8)=x_4=LABEL_{2,5}$

$F(x_4)=x_2=LABEL_{1,3}$

$F(x_2)=x_1=LABEL_{1,\phi}$

を算出することができる。

【０１８０】

なお、いずれの受信機ｕｍに対しても仮選択ラベル数と、特別なサブセットに対応しないラベルの数は同一である。図２０に示す１６個の葉（リーフ）に対応する１６個の受信機を持つ階層木の場合は、いずれの受信機ｕｍに対しても仮選択ラベル数＝１１、特別なサブセットに対応しないラベルの数＝６となる。

【０１８１】

上述のように、本発明の方式に従ったラベル提供処理では、特別なサブセットに対応するラベルのうち、一方向木において受信機ｕｍが割り当てられた葉ｙの値x_yに対応するラベルは必ず与えられ、この葉からルートへのパスを、１段ずつ左に上がるか右に上がるかと表したときに、左に上がった先のノードの値に対応するラベルがｕｍに与えられることになる。

【０１８２】

このように、各受信機ｕｍに対応するパスｍ（ｐａｔｈ－ｍ）にいくつの左上がりのパスが含まれるかによって、受信機ｕｍに与えられる特別なサブセットに対応するラベルの個数が変化する。この一方向木が、葉の数Ｎの完全２分木であるため、すべての受信機のパスｍ（ｐａｔｈ－ｍ）を考えると、左上がりのパスを１、右上がりのパスを０と表した

ときに、ｌｏｇＮ桁（ビット）の数が００...０から１１...１まで１つずつ現れる。すなわち、パスｍ（ｐａｔｈ－ｍ）のビット表現は、

｛０，１｝$^{log N}$

で表せる。

【０１８３】

例として、図１９に示す１６個の受信機ｕ１～ｕ１６に対応するパスｍ（ｐａｔｈ－ｍ）のビット表現を図２１に示す。

【０１８４】

例えば、受信機ｕ１からルートへのパス１（ｐａｔｈ－１）は、［００００］となる。図１９を参照して説明すると、受信機ｕ１からルートへのパス１（ｐａｔｈ－１）は、すべて右上がりのパス４個（１６→８，８→４，４→２，２→１）によって設定されるので、右上がりのパスを０と表した設定では、受信機ｕ１からルートへのパス１（ｐａｔｈ－１）は、［００００］となる。

【０１８５】

受信機ｕ２からルートへのパス２（ｐａｔｈ－２）は、［１０００］となる。図１９を参照して説明すると、受信機ｕ２からルートへのパス２（ｐａｔｈ－２）は、最初のみが、左上がりのパス（１７→８）であり、残りは、すべて右上がりのパス３個（８→４，４→２，２→１）によって設定されるので、受信機ｕ２からルートへのパス２（ｐａｔｈ－２）は、［１０００］となる。

【０１８６】

以下、同様に、図１９に示す１６個の受信機ｕ１～ｕ１６に対応するパスｍ（ｐａｔｈ－ｍ）のビット表現が決定される。

【０１８７】

図２１は、図１９に示す１６個の受信機ｕ１～ｕ１６に対応するパスｍ（ｐａｔｈ－ｍ）のビット表現を示す図である。図２１に示すように、受信機ｕ１～ｕ１６に対応するパスｍ（ｐａｔｈ－ｍ）のビット表現は、受信機毎に異なる［００００］～［１１１１］の１６種類のビット表現となる。

【０１８８】

パスｍ（ｐａｔｈ－ｍ）のビット表現におけるビット値［１］の数をパスｍ（ｐａｔｈ－ｍ）の［重み］と定義する。

【０１８９】

本発明の構成では、受信機ｕｍに提供されるラベルは、特別なサブセットに対応しないラベルと、特別なサブセットに対応するラベルからさらに再選択されたラベルであり、特別なサブセットに対応し再選択されるラベルは以下のラベルとなる。

【０１９０】

葉（リーフノード）のノード番号ｙに対応する値x_yに対応するラベル、すなわち、

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

が１つ必ず、受信機に与えられる。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。

【０１９１】

さらに、上受信機ｕｍに対応するパスｍ（ｐａｔｈ－ｍ）のビット表現における重みの個数（１の数）のラベルが受信機に与えられる。ここで、葉に割り当てられた値に対応するラベルは、他の値から導出されることはないので、必ず受信機に直接与えられる必要があることに注意されたい。

【０１９２】

例えば、図１９（ａ）に示す２分木構成とし、図２１に示すような各受信機ｕｍに対応するパスｍ（ｐａｔｈ－ｍ）のビット表現が設定される構成において、パスｍ（ｐａｔｈ－ｍ）のビット表現がオール０である受信機ｕ１には、受信機ｕ１に対応する葉（ノード番号＝１６）に対応するノード対応値x_{16}に対応するラベル$x_{16} = LABEL_{8,17}$のみが与えられ、その他のラベルは与えられない。

【０１９３】
ビット表現に含まれる１が１つだけ含むｌｏｇＮ個の受信機（ｕ２，ｕ３，ｕ５，ｕ９）には、受信機ｕｍの設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて１つのラベルが与えられる。ただし、ここで受信機が割り当てられた葉を「自己ノード」と呼んでいる。
【０１９４】
以下同様であり、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて、ラベルをｊ個（ｊ＝０，１，...，ｌｏｇＮ）与えられる受信機の数は、下式
【数３】

$$\binom{\log N}{j}$$

で表される。
なお、上記式は、ｌｏｇＮ個からｊ個を選択する場合の数を示す式である。
【０１９５】
具体的には、図１９に示す２分木構成（Ｎ＝１６）において、
ｌｏｇ１６＝４である。
ｊ＝１の場合、すなわち、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて、さらに１個のラベルを与えられる受信機は、（ｕ２，ｕ３，ｕ５，ｕ９）の４つとなる。
ｊ＝２の場合、すなわち、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて、さらにラベルを２個与えられる受信機は、（ｕ４，ｕ６，ｕ７，ｕ１０，ｕ１１，ｕ１３）の６つとなる。
ｊ＝３の場合、すなわち、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて、さらにラベルを３個与えられる受信機は、（ｕ８，ｕ１２，ｕ１４，ｕ１５）の４つとなる。
ｊ＝４の場合、すなわち、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて、さらにラベルを４個与えられる受信機は、（ｕ１６）の１つとなる。
なお、ノードｕ１は自己ノードに対応するノード対応値対応のラベルのみを保有すればよい。
【０１９６】
このように、本発明のノードキー設定処理を行なった構成では、各葉（リーフ）に対応付けられた受信機は、特別なサブセット対応のラベルについては、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えてｊ個、つまりトータルでｊ＋１個のラベルを保持すればよい。ただし、ｊは前述の条件（ｂ１）（ｂ２）を共に満たすリーフ以外のノードｉの個数であり、パスｍ（ｐａｔｈ－ｍ）に含まれるリーフ以外のノードの数はｌｏｇＮで

あるため、ｊは０以上ｌｏｇＮ以下の数となる。

【０１９７】

従来のＳｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式では、各受信機に与えられる特別サブセット対応のラベルは、受信機数をＮとした場合、

ｌｏｇＮ＋１個

である。

【０１９８】

ＳＤ方式において受信機に与えられる特別なサブセットに対応するラベルの数は、以下のようにして算出される。ある受信機が属する、ノードｉ、ｊが親子関係になっている、第１の特別なサブセット$S_{i,j}$は、その受信機が割り当てられた葉からルートまでのパス上の内部ノードの数だけ存在する。内部ノードがｉとなり、その子ノードのうち上記のパス上にないほうのノードがｊとなるからである。

【０１９９】

よって、ある受信機が持つ、第１の特別なサブセットに対応するラベルの個数はｌｏｇＮとなる。また、第２の特別なサブセット$S_{1,\phi}$は、リボークする受信機がない場合に用いられるものであり、全受信機が属している。すなわち、全受信機が$LABEL_{1,\phi}$を持っている。以上から、ＳＤ方式において受信機に与えられる特別なサブセットに対応するラベルの数はｌｏｇＮ＋１個となる。

【０２００】

一方、本方式では、受信機数をＮとした場合、各受信機に与えられる特別サブセット対応のラベルの数は、上述したように、

ｊ＋１個

である。

【０２０１】

従って、本方式を適用することにより、各受信機が保持するラベル数を下記の数、削減することが可能となる。すなわち、

（ｌｏｇＮ＋１）－（ｊ＋１）

＝ｌｏｇＮ－ｊ個

の削減が可能となる。

【０２０２】

この削減された分のラベルは、各受信機が保持するラベルに対して一方向性関数Ｆを適用することによって取得することができる。

【０２０３】

ところで、下記式

【数４】

$$\binom{\log N}{j}=\binom{\log N}{\log N-j}$$

である点に注意されたい。すなわち、受信機数Ｎの２分木構成において、ラベル数をｊ個削減することのできる受信機の数も、

【数５】

$$\binom{\log N}{j}$$

によって示されることになる。

【０２０４】

上述したセットアップ処理のフローを図２２に示す。図２２のフローの各ステップについて説明する。

【０２０５】

まず、ステップＳ２０１において、管理センタ（ＴＣ）は、Ｎ個の葉を持つ２分木を定義する。２分木における最上位ノードであるルートを１とし、以降を幅優先（ｂｒｅａｄｔｈ　ｆｉｒｓｔ　ｏｒｄｅｒ）で番号設定を行う。すなわち、図１９、図２０に示すような階層木の各ノードについてノード対応番号の設定を行なう。

【０２０６】

さらに、受信機ｕｍ（ｍ＝１，２，...，Ｎ）を木の各葉（リーフ）に割り当てる。また、Ｃビット出力の一方向関数Ｆを選択して公開する。Ｃは任意の数であり、一方向性関数は、例えばＭＤ４、ＭＤ５、ＳＨＡ－１など既存の一方向性関数（ハッシュ関数）の適用が可能である。

【０２０７】

さらに、Ｎ個の葉を持つ２分木においてサブセットを定義する。これは、先に図６を参照して説明したように、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」を表すサブセットを定義する。

【０２０８】

次にステップＳ２０３において、管理センタ（ＴＣ）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、葉がＮ個である２分木における各ノードｉの対応値x_iとして設定した一方向木を構成する。すなわち、

（ａ）２分木を構成する葉（リーフ）の数Ｎ、

（ｂ）Ｃビット出力の一方向性関数Ｆ、

を入力として、２分木を構成する全ノード（葉（リーフ）を含む）数：２Ｎ－１に対応する２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}

を決定する。

【０２０９】

管理センタ（ＴＣ）は、決定した２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}を、ステップＳ２０１で定義したサブセット中の、特別サブセットに対応するラベルとして決定する。

【０２１０】

すなわち、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Ｃビットの数x_1，x_2，...，x_{2N-1}中の１つの値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$SS_{1,\phi}$のラベルとし、その他のx_2，...，x_{2N-1}の値を、、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$_{i,j}$として設定する。すなわち、

ＬＡＢＥＬ$_{1,\phi}$＝ｘ$_{1}$

と設定し、

さらに、ｙ＝１，２，...，Ｎ－１に対して、

ＬＡＢＥＬ$_{y,2y}$＝ｘ$_{2y+1}$

ＬＡＢＥＬ$_{y,2y+1}$＝ｘ$_{2y}$

とする。

【０２１１】

次に、ステップＳ２０３において、特別なサブセットに対応しないラベルを導出する。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。

【０２１２】

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。

【０２１３】

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。

【０２１４】

次に、ステップＳ２０４において、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。これは、前述したように、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。

【０２１５】

次に、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。管理センタ（ＴＣ）は、仮選択ラベルのうち以下の条件（ａ）を満足するラベルと、以下の条件（ｂ）を満足するラベルをそれぞれ選択して、各受信機ｕｍに対する最終的な提供ラベルとして決定する。

【０２１６】

（ａ）仮選択ラベル中、いずれの特別なサブセットにも該当しないもの、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$_{i,j}$、および、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$_{1,\phi}$のいずれでもないサブセット対応のラベルＬＡＢＥＬ$_{i,}$

ｊ。
（ｂ）仮選択ラベル中、いずれか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$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれかに対応するラベルであり、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
である値ｙに対応する値x_yに対応するラベル$LABEL_{i,j}$。
上記（ａ）の条件を満足するラベルと、（ｂ）の条件を満足するラベルとを、受信機ｕｍに対する最終提供ラベルとして決定し、受信機に提供する。

【０２１７】
（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。

【０２１８】
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。

【０２１９】
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。

【０２２０】
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。

【０２２１】
図２３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２３に示す２つのサブセット$S_{2,20}$と$S_{3,13}$である。

【０２２２】
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。

【０２２３】
情報配信処理の処理手順について、図２４に示すフローを参照して説明する。図２４に

示すフロー中の各ステップについて説明する。

【０２２４】

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。

【０２２５】

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２３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。

【０２２６】

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２３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。

【０２２７】

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２３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２３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。

【０２２８】

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。

【０２２９】

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。

【０２３０】

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。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。

【０２３１】

（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。

【０２３２】

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が、受信機がラベルＬＡＢＥＬ$_{i,k}$を直接保持しないもの（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の子孫であるが、受信機がラベルＬＡＢＥＬ$_{i,k}$を直接保持しないもの）

のいずれであるかを判断する。

【０２３３】

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受信機がラベルＬＡＢＥＬ$_{i,\phi}$を保持していれば（Ａ）であるとし、そうでなければ（Ｂ）であるとみなす。なお、このケースにおいて、（Ｂ）の場合には、受信機は、自己の保持する特別サブセット対応のラベルに対する一方向性関数Ｆの適用によりラベルＬＡＢＥＬ$_{i,\phi}$を算出することができる。

【０２３４】

（Ｂ）の場合には、下記のように、受信機に与えられているラベルに基づいて、暗号文に適用されているサブセットキーを導出するためのラベルＬＡＢＥＬ$_{i,k}$を算出する。

【０２３５】

まず、受信機ｕｍは、ＬＡＢＥＬ$_{i,k}$に対応する一方向木のノードｙ（すなわちＬＡＢＥＬ$_{i,k}$＝ｙ）を見つける。そして、$2^n y$は、受信機ｕｍに対応するパスノードｍ（ＰａｔｈＮｏｄｅｓ－ｍ）に含まれるが、$2^{n+1} y$は、パスノードｍ（ＰａｔｈＮｏｄｅｓ－ｍ）に含まれない最小のｎを検出する。このとき、受信機ｕｍは、ノード$2^n y$の対応値、

【数６】

$$x_{2^n y}$$

に対応するラベルを保持している。なお、ここで、ｎ＝０ならば、受信機ｕｍは、値ｘ$_y$に対応するラベルを直接保持しているので、上記（Ａ），（Ｂ）の条件の（Ａ）に対応することになる。よってここではｎ＞０となる。

【０２３６】

受信機は、上記処理によって検出したノード$2^n y$の対応値、

【数７】

$$x_{2^n y}$$

に等しい値を持つラベルに対して一方向性関数Ｆをｎ回適用することで、ノードｙの値ｘｙに対応するＬＡＢＥＬ$_{i,k}$を算出する。

【０２３７】

このようにして、サブセットＳ$_{i,k}$に対応するＬＡＢＥＬ$_{i,k}$を導出したら、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。

【０２３８】

具体的なサブセットキーの導出処理例について、図２５を参照して説明する。図２５に示すように、受信機ｕ５，ｕ１１，ｕ１２がリボークされ、サブセットＳ$_{2,20}$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。

【０２３９】

まず、受信機ｕ４（ノード番号＝１９）における処理例を説明する。受信機ｕ４は、特別サブセットに対応するラベル：ＬＡＢＥＬ$_{2,5}$，ＬＡＢＥＬ$_{4,8}$、ＬＡＢＥＬ$_{9,18}$の３個のラベルと、特別サブセットに対応しないラベル：ＬＡＢＥＬ$_{1,5}$，ＬＡＢＥＬ$_{1,8}$，ＬＡＢＥＬ$_{1,18}$，ＬＡＢＥＬ$_{2,8}$，ＬＡＢＥＬ$_{2,18}$，ＬＡＢＥＬ$_{4,18}$，の６個のラベルとの計９個のラベルを保持している。

【０２４０】

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$_{2,20}$に対し、ノード２０の先祖であるノード５を用いたラベルＬＡＢＥＬ$_{2,5}$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（この場合、３回）だけ適用することでサブセットキーＳＫ$_{2,20}$を得ることができる。

【０２４１】

前述したように、従来のＳＤ方式では、受信機ｕ４に対しては、

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個のラベルが提供されることになるが、本発明の方式においては、上述したように、受信機ｕ４には、９個のラベル、すなわち、

特別サブセット非対応ラベルとして、

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、

特別サブセット対応ラベルとして、

$x_4 = LABEL_{2,5}$、$x_9 = LABEL_{4,8}$、$x_{16} = LABEL_{9,18}$の３個のラベル、

のみが提供されることになる。

【０２４２】

本発明の方式において、受信機ｕ４に付与されない２つのラベルは、
$LABEL_{1,3}$、
$LABEL_{1,\phi}$、
の２つのラベルであり、
これらのラベルについては、受信機ｕ４は、提供されたラベルから算出する。すなわち、
$LABEL_{1,3}=x_2$
$LABEL_{1,\phi}=x_1$
であり、
受信機ｕ４は、$x_4=LABEL_{2,5}$を有しており、
前述したノード対応値としての２Ｎ－１個のＣビットの数$x_1, x_2, \ldots, x_{2N-1}$のそれぞれは、前述の図１４のフローを参照して説明したアルゴリズムに従って算出される値であり、
$F(x_i)=x_{i/2}$
を満足する。

【０２４３】

従って、受信機ｕ４は、所有するラベル$x_4=LABEL_{2,5}$に基づいて、
$F(x_4)=x_2=LABEL_{1,3}$
$F(x_2)=x_1=LABEL_{1,\phi}$
を算出することができる。

【０２４４】

従って、受信機ｕ４は、所有するラベル数は従来のＳＤ方式より、少なくなるが、利用可能なラベル数は従来のＳＤ方式と同様となる。

【０２４５】

次に、受信機ｕ１（ノード番号＝１６）における処理例を説明する。受信機ｕ１は、図２６に示すように、特別サブセットに対応するラベル：$LABEL_{8,17}$の１個のラベルと、特別サブセットに対応しないラベル：$LABEL_{1,5}$，$LABEL_{1,9}$，$LABEL_{1,17}$，$LABEL_{2,9}$，$LABEL_{2,17}$，$LABEL_{4,17}$，の６個のラベルとの計７個のラベルを保持している。

【０２４６】

この場合、受信機ｕ１は、上記（Ｂ）に相当する。すなわち、（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が、受信機がラベル$LABEL_{i,k}$を直接保持しないもの（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の子孫であるが、受信機がラベル$LABEL_{i,k}$を直接保持しないもの）である。

【０２４７】

具体的には、受信機ｕ１は、サブセット$S_{2,20}$に対してノード２０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、保持しているラベル$LABEL_{8,17}$から、$LABEL_{2,5}$を導出する。

【０２４８】

従来の、オリジナルのＳＤ方式において受信機ｕ１に付与されるラベルは、
$LABEL_{1,3}$、$LABEL_{1,5}$、$LABEL_{1,9}$、$LABEL_{1,17}$、$LABEL_{2,5}$、$LABEL_{2,9}$、$LABEL_{2,17}$、$LABEL_{4,9}$、$LABEL_{4,17}$、$LABEL_{8,17}$、$LABEL_{1,\phi}$の１１個のラベルが提供されることになるが、本発明の方式においては、上述したように、受信機ｕ１には、７個のラベルのみが提供されることになる。

【０２４９】

本発明の方式において、受信機ｕ１に付与されない４つのラベルは、

$LABEL_{4,9}$、
$LABEL_{2,5}$、
$LABEL_{1,3}$、
$LABEL_{1,\phi}$、
の４つのラベルであるが、
これらのラベルについては、受信機ｕ１は、提供されたラベルから算出する。すなわち、
$LABEL_{4,9}=x_8$、
$LABEL_{2,5}=x_4$、
$LABEL_{1,3}=x_2$
$LABEL_{1,\phi}=x_1$
であり、
受信機ｕ１は、$x_{16}=LABEL_{8,17}$を有しており、
前述したノード対応値としての２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}のそれぞれは、前述の図１４のフローを参照して説明したアルゴリズムに従って算出される値であり、
$F(x_i)=x_{i/2}$
を満足する。

【０２５０】

従って、受信機ｕ１は、所有するラベル$x_{16}=LABEL_{8,17}$に基づいて、
$F(x_{16})=x_8=LABEL_{4,9}$
$F(x_8)=x_4=LABEL_{2,5}$
$F(x_4)=x_2=LABEL_{1,3}$
$F(x_2)=x_1=LABEL_{1,\phi}$
を算出することができる。

【０２５１】

図２６の例では、$LABEL_{2,5}$を導出することが求められるので、受信機ｕ１は、受信機ｕ１の保持する特別サブセット対応ラベル$x_{16}=LABEL_{8,17}$に対して、一方向性関数Ｆを２回適用して、$LABEL_{2,5}$を導出する。

【０２５２】

この導出したラベル$LABEL_{2,5}$に擬似乱数生成器Ｇを必要な回数（３回）適用することで、暗号文に適用されているサブセットキー$SK_{2,20}$を算出することができる。

【０２５３】

この処理は、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も同様である。すなわち、受信機は$LABEL_{1,\phi}$を直接保持しているか、一方向性関数Ｆを必要な回数だけ適用して$LABEL_{1,\phi}$を導出可能なラベルを保持しているため、後者の場合には関数Ｆを用いて$LABEL_{1,\phi}$を求める。そして、$SK_{1,\phi}=G_M(LABEL_{1,\phi})$によりサブセットキーを求める。なお、$LABEL_{1,\phi}$からはそれ以外のラベルを導出することはないので、サブセットキー$SK_{1,\phi}$だけ特別に、$SK_{1,\phi}=LABEL_{1,\phi}$と定めれば、リボークする受信機がない場合に擬似乱数生成器Ｇの適用回数を１回減らすことができ、負荷の軽減につながる。

【０２５４】

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２７のフローチャートを参照して説明する。

【０２５５】

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。

【０２５６】

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。

【０２５７】

サブセットキーの導出処理において、受信機は、以下の処理を実行する。

（１）暗号文の適用サブセットキーが、特別サブセット対応のラベルから擬似乱数生成処理により算出可能なサブセットキーでない場合、受信機は自己の保持する特別サブセット非対応のラベルに対して擬似乱数生成器Ｇを必要な回数適用して、暗号文の適用サブセットキーを算出する。

（２）暗号文の適用サブセットキーが、特別サブセット対応のラベルから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る場合は、受信機は自己の保持する特別サブセット対応のラベルから擬似乱数生成器Ｇのみで暗号文の適用サブセットキーを算出可能か否かを判断し、

（２－１）可能な場合は、特別サブセット対応のラベルに対して、擬似乱数生成器を必要な回数適用して、暗号文の適用サブセットキーを算出する。

（２－２）不可能な場合は、自己の保持する特別サブセット対応のラベルに対して、一方向性関数Ｆを必要な回数適用し、新たな特別サブセット対応のラベルを算出し、算出した新たな特別サブセット対応のラベルに対して、擬似乱数生成器を必要な回数適用して、暗号文の適用サブセットキーを算出する。

【０２５８】

（２－２）におけるラベル算出処理は、階層木において、受信機ｕｍ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処理として行なわれる。受信機ｕｍの有する階層木の下位の特別サブセット対応のラベルからより上位の特別サブセット対応のラベルが一方向性関数の適用により算出される。

【０２５９】

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。

【０２６０】

次に、図２８、図２９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。

【０２６１】

まず、図２８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、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。

【０２６２】

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、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、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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定したラベルを生成する。一方向性関数Ｆは、例えばＭＤ４またはＭＤ５またはＳＨＡ－１が適用可能である。

【０２６３】

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。

【０２６４】

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、選択された特別サブセットに対応するラベルの値を、特別サブセットの直下に設定される他の特別サブセットの値に対する一方向性関数Ｆの適用によって算出可能としたラベルを生成する。

【０２６５】

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、末端ノード数Ｎの２分木構成を持つ階層木においてＮ個の値：x_N～x_{2N-1}を決定し、ｉ＝２Ｎ－１とする初期設定を実行し、ｉ＝（２Ｎ－１）～１において、ｉ＝偶数の場合に、一方向性関数Ｆを適用しＦ（x_i）を計算し、これを$x_{i/2}$とセットし、この各処理によって、末端ノード数Ｎの２分木構成において、２Ｎ－１個の特別サブセット対応のラベルの値：x_1～x_{2N-1}を決定する。

【０２６６】

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であって、受信機に提供されるラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルとを受信機に対する提供ラベルとして決定する。

【０２６７】

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、下記条件、
（ａ）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$SS_{i,j}$、および、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$SS_{1,\phi}$のいずれでもないサブセット対応のラベル$LABEL_{i,j}$と、
（ｂ）仮選択ラベルから、前記第１の特別なサブセット$SS_{i,j}$、および、前記第２の特別なサブセット$SS_{1,\phi}$のいずれかに対応するラベルであり、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
である値ｙに対応する値x_yに対応するラベル$LABEL_{i,j}$と、
上記（ａ）または（ｂ）の条件を満足するラベルを、受信機ｕｍに対する最終提供ラベルとして決定する。

【０２６８】

提供ラベル決定手段４１２は、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［x_y＝$LABEL_{P(y),S(y)}$］に加えてｊ個のラベル、（ただし、ｊは０以上ｌｏｇＮ、Ｎは、前記階層木における末端ノード数＝受信機数）、を受信機に対する特別サブセット対応の提供ラベル数として決定する。

【０２６９】

暗号文生成手段４１３は、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。

【０２７０】

次に、図２９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。

【０２７１】

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。

【０２７２】

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。

【０２７３】

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、保持ラベルに対して一方向性関数Ｆを適用し、保持ラベルと異なるラベルを算出する。

【０２７４】

ラベル算出手段４２２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、この特別サブセット対応のラベルを保持していない場合に、保持している他のラベルに対する一方向性関数Ｆの適用により、この特別サブセット対応のラベルを算出する。

【０２７５】

ラベル算出手段４２２は、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を一方向性関数による演算を実行して算出する。適用する方向性関数Ｆは、ＭＤ４またはＭＤ５またはＳＨＡ－１などである。

【０２７６】

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において他の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。

【０２７７】

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。

【０２７８】

図３０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。

【０２７９】

情報処理装置５００は、図３０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。

【０２８０】

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。

【０２８１】

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。

【０２８２】

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、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。

【０２８３】

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）と、特別サブセット非対応のラベル（ＬＡＢＥＬ）とが格納される。

【０２８４】

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に格納される特別サブセット対応のラベル（ＬＡＢＥＬ）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、

から構成される特別サブセットから選択されたサブセットに対応のラベルであり、自己の保持するラベルから算出することが不可能な最小の個数のラベルである。

【０２８５】

すなわち、前述したように、受信機は、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（X_y）に相当するラベル［$x_y = LABEL_{P(y),S(y)}$］に加えて、ラベルをｊ個（ｊ＝０，１，...，ｌｏｇＮ）格納することになる。

【０２８６】

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。

【０２８７】

［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。

【０２８８】

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。

【０２８９】

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。

【０２９０】

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３１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３１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。

【０２９１】

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３１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。

【０２９２】

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。

【０２９３】

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。

【０２９４】

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３２を参照して説明する。図３２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、$LABEL_{1,3}$，$LABEL_{1,5}$，ＬＡ

ＢＥＬ$_{1,8}$，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。

【０２９５】

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８】

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

となる。

【０２９６】

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９】

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

である。

【０２９７】

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１０】

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

である。

【０２９８】
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１１】

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

である。
【０２９９】
［７．一方向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$LABEL_{i,j}$を別のラベルから一方向性関数Ｆを適用して導出可能とすることで、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。
【０３００】
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。
【０３０１】
図３２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３３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３２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サブセット対応のラベル$LABEL_{1,\phi}$の合計９個のラベルを保持しておく必要があった。
【０３０２】
これに対し、本発明では、上記９個のラベル中、特別サブセット非対応の４個のラベル$LABEL_{1,5}$，$LABEL_{1,8}$，$LABEL_{1,18}$，$LABEL_{4,18}$と、特別サブセット対応のラベルであり、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれるノードであり、かつ、
（ｂ２）ノード２ｙがＰａｔｈＮｏｄｅｓ－ｍに含まれていないノード
である値ｙに対応する値x_yに対応するラベル$LABEL_{i,j}$。
のみを保持すればよい。
【０３０３】
図３２の例における受信機ｕ４において、

（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれ、
の条件を満足するノードは、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝の各ノードである。
この中で、
（ｂ２）ノード２ｙが含まれていないノード
は、ノード４，９，１９となる。ノード１，２については、
ノード１は、ノード２×１に対応するノード２が、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝中に含まれ、また、
ノード２は、ノード２×２に対応するノード４が、ＰａｔｈＮｏｄｅｓ－４＝｛１，２，４，９，１９｝中に含まれる。

【０３０４】
従って、受信機ｕ４において、
（ｂ１）ノードｙがＰａｔｈＮｏｄｅｓ－ｍに含まれ、かつ、
（ｂ２）ノード２ｙが含まれていないノード
これらの条件（ｂ１），（ｂ２）を満足するノードは、ノード番号はｙ＝４，９，１９となる。

【０３０５】
この結果、ｙ＝４，９，１９に対応するノード対応値x_4，x_9，x_{19}に対応するラベル、すなわち、
$x_4 = LABEL_{2,5}$
$x_9 = LABEL_{4,8}$
$x_{19} = LABEL_{9,18}$
が、条件（ｂ）を満足するラベルとして選択され、これらの３つのラベルが、受信機ｕ４に対する提供ラベルとして決定される。

【０３０６】
結果として、受信機ｕ４には、
特別サブセット非対応のラベルとして、
$LABEL_{1,5}$、$LABEL_{1,8}$、$LABEL_{1,18}$、$LABEL_{4,18}$の４個のラベル、
特別サブセット対応のラベルとして、
$x_4 = LABEL_{2,5}$、$x_9 = LABEL_{4,8}$、$x_{19} = LABEL_{9,18}$の３個のラベル、
計７個のラベルが提供されるラベルとなる。

【０３０７】
本発明の方式において、受信機ｕ４に付与されない２つのラベルは、
$LABEL_{1,3}$、
$LABEL_{1,\phi}$、
の２つのラベルであるが、
これらのラベルについては、受信機ｕ４は、提供されたラベルから算出する。すなわち、
$LABEL_{1,3} = x_2$
$LABEL_{1,\phi} = x_1$
であり、
受信機ｕ４は、$x_4 = LABEL_{2,5}$を有しており、
前述したノード対応値としての２Ｎ－１個のＣビットの数x_1，x_2，...，x_{2N-1}のそれぞれは、前述の図１４のフローを参照して説明したアルゴリズムに従って算出される値であり、
$F(x_i) = x_{i/2}$
を満足する。

【０３０８】

従って、受信機ｕ４は、所有するラベルｘ$_4$＝ＬＡＢＥＬ$_{2,5}$に基づいて、
Ｆ（ｘ$_4$）＝ｘ$_2$＝ＬＡＢＥＬ$_{1,3}$
Ｆ（ｘ$_2$）＝ｘ$_1$＝ＬＡＢＥＬ$_{1,\phi}$
を算出することができる。

【０３０９】

このように、ベーシックＬＳＤ方式においても本発明の一方向木を適用した構成により、受信機の保持ラベル数を削減することができる。

【０３１０】

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。

【０３１１】

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。

【０３１２】

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。

【０３１３】

すなわち、ベーシックＬＳＤ方式においても、前述したＳＤ方式と同様の個数のラベル数の削減が実現される。具体的には、ベーシックＬＳＤ方式においても、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（Ｘ$_y$）に相当するラベル［ｘ$_y$＝ＬＡＢＥＬ$_{P(y),S(y)}$］に加えて、ラベルをｊ個（ｊ＝０，１，...，ｌｏｇＮ）与えられ、受信機数をＮとした場合、各受信機に与えられる特別サブセット対応のラベルの数は、

ｊ＋１個

である。

【０３１４】

本発明の方式を適用することにより、受信機Ｎ個のうち、

【数１２】

$$\begin{pmatrix} \log N \\ j \end{pmatrix}$$

の個数の受信機においてラベル数をｊ個削減することが可能となる。

【０３１５】
この削減された分のラベルは、各受信機が保持するラベルに対して一方向性関数Ｆを適用することによって取得することができる。
【０３１６】
［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。
【０３１７】
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。
【０３１８】
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。
【０３１９】
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１３】

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

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。
【０３２０】
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．
【０３２１】
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。

【０３２２】

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１４】

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

となる。

【０３２３】

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１５】

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

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。

【０３２４】

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。

【０３２５】

［９．一方向木を用いた一般化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、一方向木を利用する部分に違いはない。

【０３２６】

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特別サブセット対応のラベルはｌｏｇＮ個ある。これらのラベルの少なくとも一部を他の特別サブセット対応のラベルに対して一方向性関数Ｆを適用して算出可能とすることにより、受信機の保持すべきラベル数の削減が可能となる。

【０３２７】

すなわち、一般化ＬＳＤ方式においても、前述したＳＤ方式と同様の個数のラベル数の削減が実現される。具体的には、一般化ＬＳＤ方式においても、受信機の設定された自己ノード（リーフ）のノード番号（ｙ）の対応値（Ｘ$_{y}$）に相当するラベル［ｘ$_{y}$＝ＬＡＢＥＬ$_{P(y),S(y)}$］に加えて、ラベルをｊ個（ｊ＝０，１，...，ｌｏｇＮ）与えられ、受信機数をＮとした場合、各受信機に与えられる特別サブセット対応のラベルの数は、

ｊ＋１個

である。

【０３２８】

本発明の方式を適用することにより、受信機Ｎ個のうち、

【数１６】

$$\binom{\log N}{j}$$

の個数の受信機においてラベル数をｊ個削減することが可能となる。

【０３２９】

この削減された分のラベルは、各受信機が保持するラベルに対して一方向性関数Ｆを適用することによって取得することができる。

【０３３０】

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）であり、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。

【０３３１】

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。

【０３３２】

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。

【０３３３】

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。

【０３３４】

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。

【０３３５】

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】

【０３３６】

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、さらに一方向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。

【０３３７】

さらに、本発明の構成によれば、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、他の特別サブセット対応のラベルの値に対する一方向性関数Ｆの適用によって算出可能な値として設定し、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であって、受信機への提供ラベルに対する一方向性関数Ｆの適用によって算出可能なラベルを除く最小限の特別サブセット対応ラベルを受信機に対する提供ラベルとしたので、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、受信機側の保持ラベルに対する一方向性関数Ｆの適用により算出可能であり、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】

【０３３８】

【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

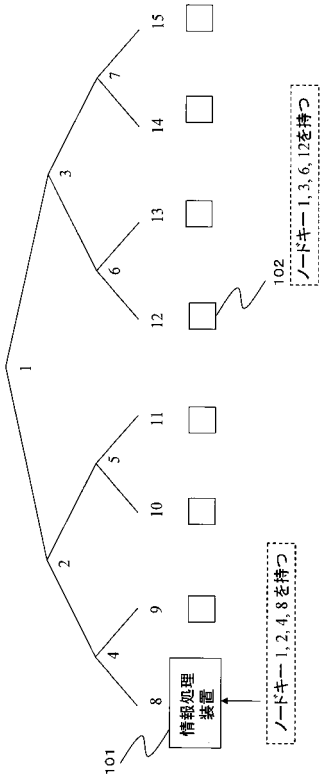
持つノードキーについて説明する図である。
【図５】ＣＳ方式において秘密情報をリボークされない受信機のみに選択的に提供するかについて説明する図である。
【図６】Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式におけるサブセットの定義について説明する図である。
【図７】Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式におけるラベルの設定および構成について説明する図である。
【図８】Ｓｕｂｓｅｔ　Ｄｉｆｆｅｒｅｎｃｅ（ＳＤ）方式におけるサブセットの設定について説明する図である。
【図９】ＳＤ方式において、全受信機数Ｎ＝１６の設定の場合に各受信機が保持すべきラベルを示す図である。
【図１０】ＳＤ方式において、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】一方向木の構成について説明する図である。
【図１４】一方向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Ｃビットの値$x_1, x_2, \ldots, x_{2N-1}$との対応を示す図である。
【図１８】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１９】各受信機ｕｍ対応のパスｍ、パスノードｍについて説明する図である。
【図２０】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２１】図１９に示す１６個の受信機ｕ１～ｕ１６に対応するパスｍ（ｐａｔｈ－ｍ）のビット表現を示す図である。
【図２２】セットアップ処理のフローを示す図である。
【図２３】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２４】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２５】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２６】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２７】受信機における暗号文の復号処理手順を説明するフロー図である。
【図２８】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２９】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３０】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３１】ベーシックＬＳＤ方式について説明する図である。
【図３２】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３３】一方向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】

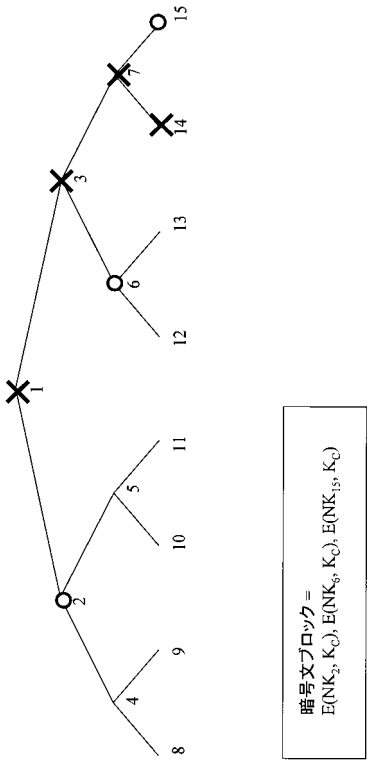
【０３３９】

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$_{P(y),S(y)}$
３２１，３２２，３２３　各受信機ｕｍ対応のパスｍ
４１０　情報処理装置
４１１　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　サブセットキー生成手段
４２４　復号手段
４２５　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

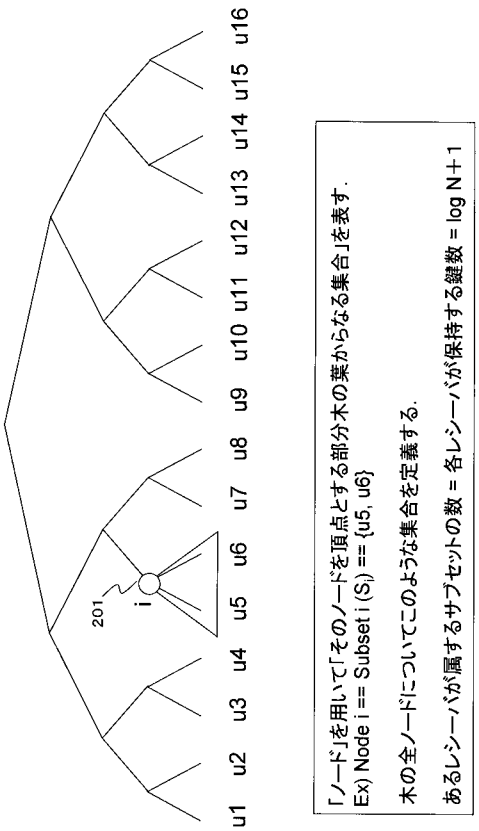
【図１】


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
101
情報処理装置
ノードキー 1, 2, 4, 8 を持つ
102
ノードキー 1, 3, 6, 12を持つ

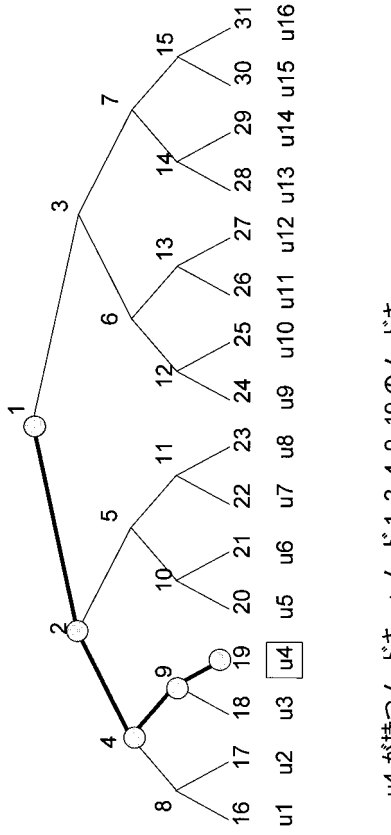
【図２】


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
暗号文ブロック =
E(NK2, KC), E(NK6, KC), E(NK15, KC)

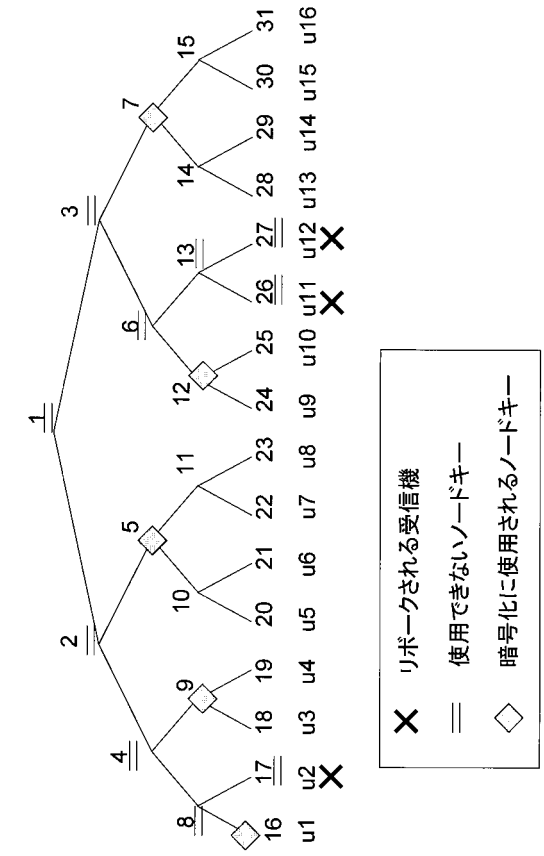
【図３】


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

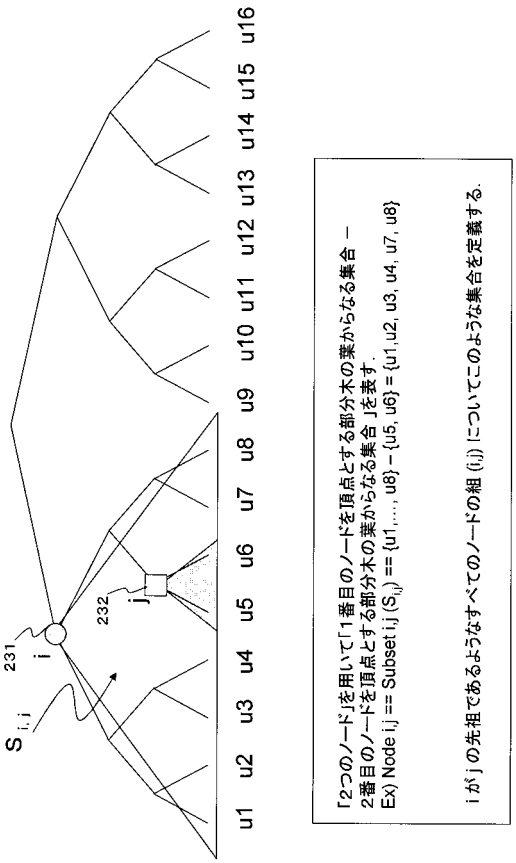
【図４】


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

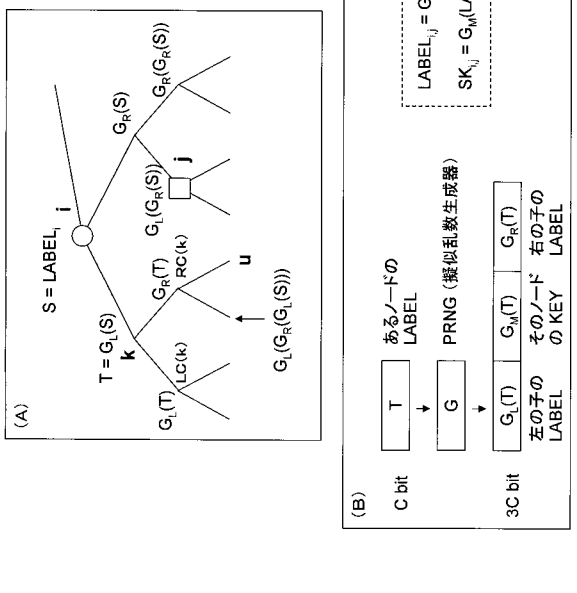
【図５】


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

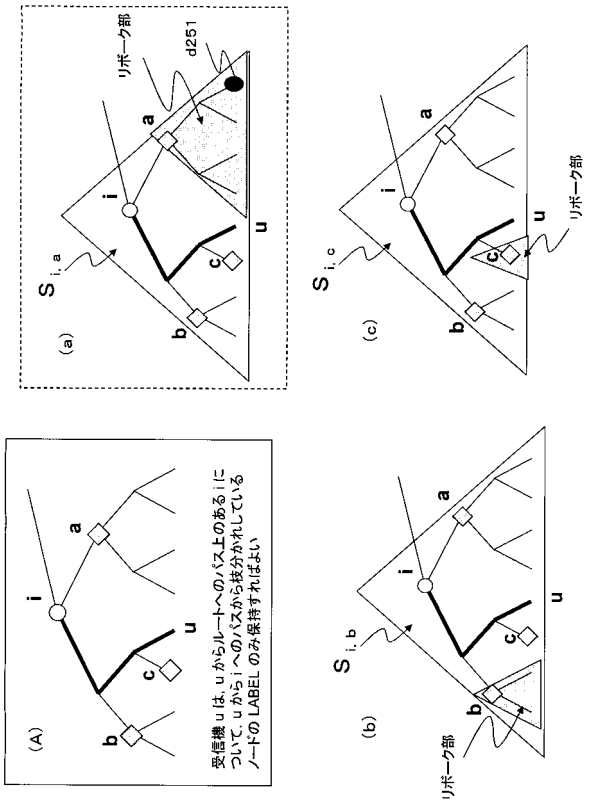
【図６】


u1 u2 u3 u4 u5 u6 u7 u8 u9 u10 u11 u12 u13 u14 u15 u16
「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 − 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} − {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.

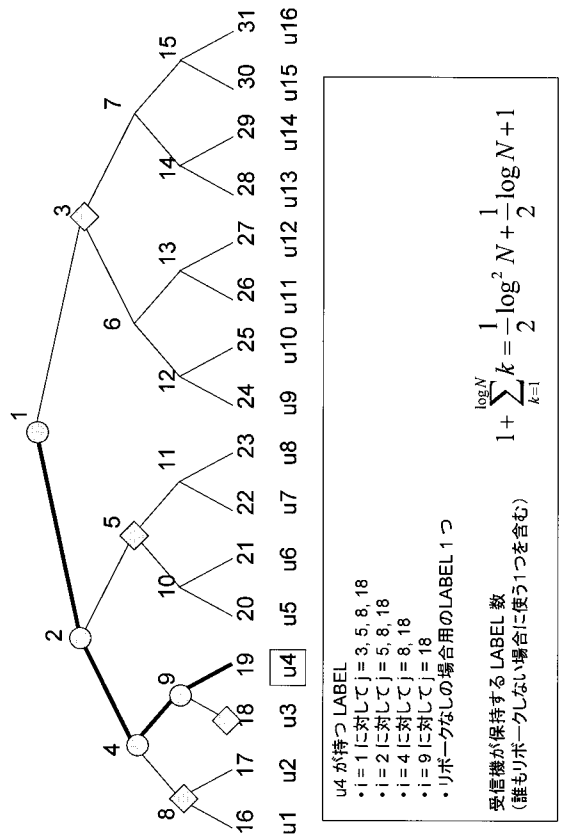
【図７】


(A)
(B)
C bit
3C bit
あるノードの LABEL
PRNG（擬似乱数生成器）
左のノードの LABEL
そのノードの KEY
右のノードの LABEL

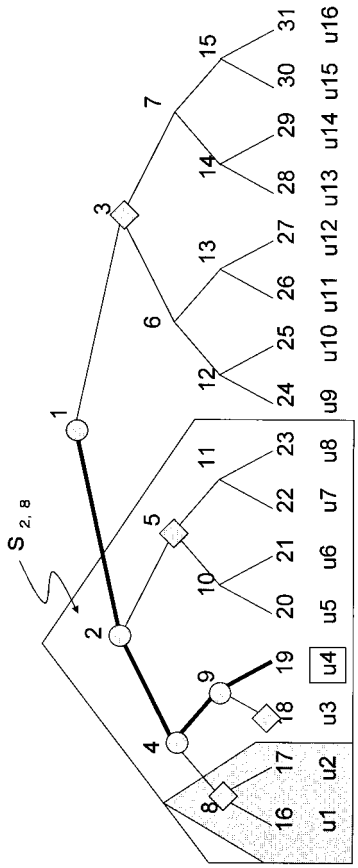
【図８】


(A)
(a)
(b)
(c)
リボーク部
d251
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

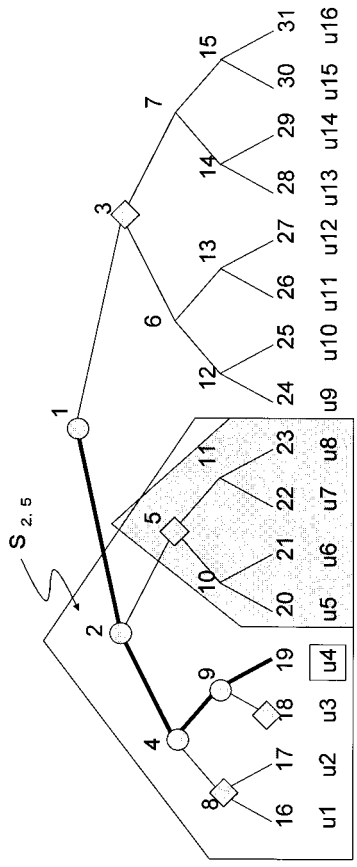
【図９】



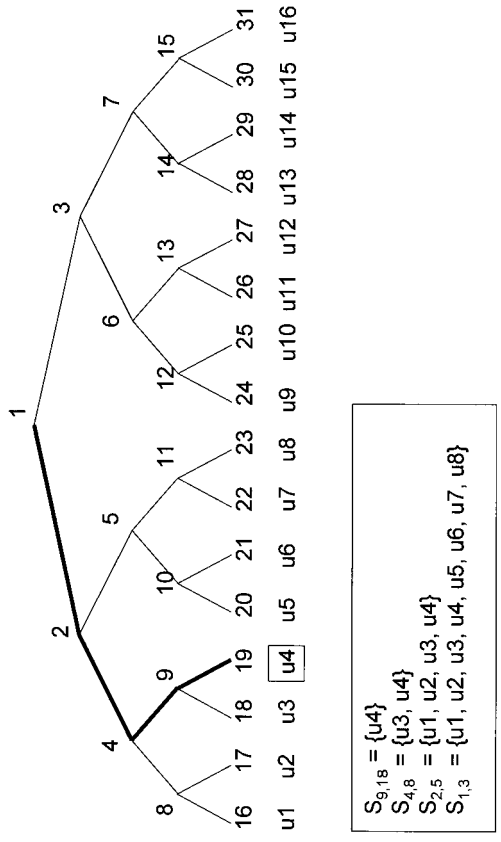
【図１０】



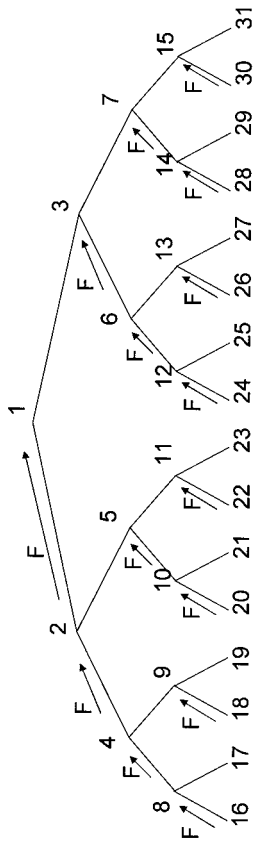
【図１１】



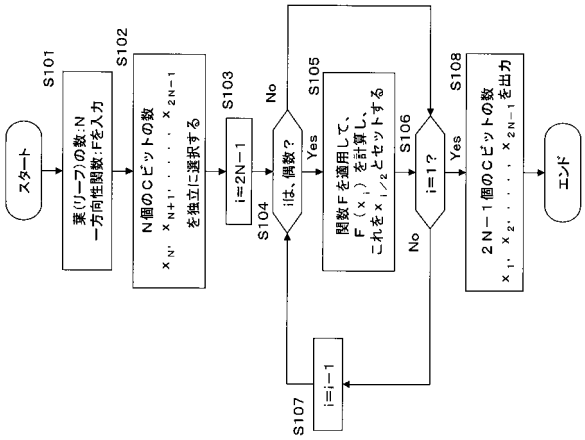
【図１２】



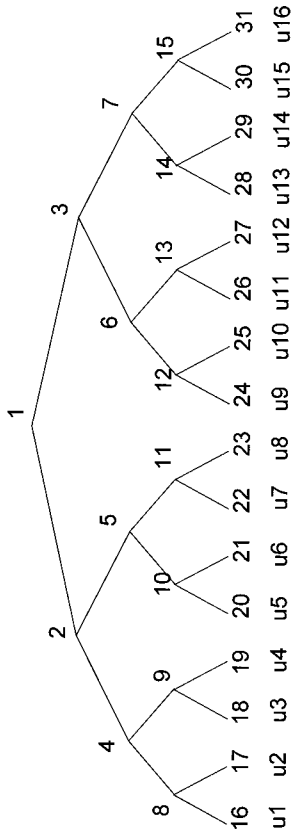
【図１３】



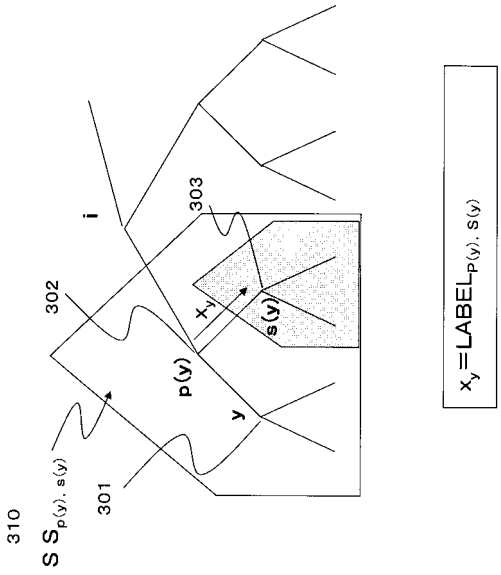
【図１４】



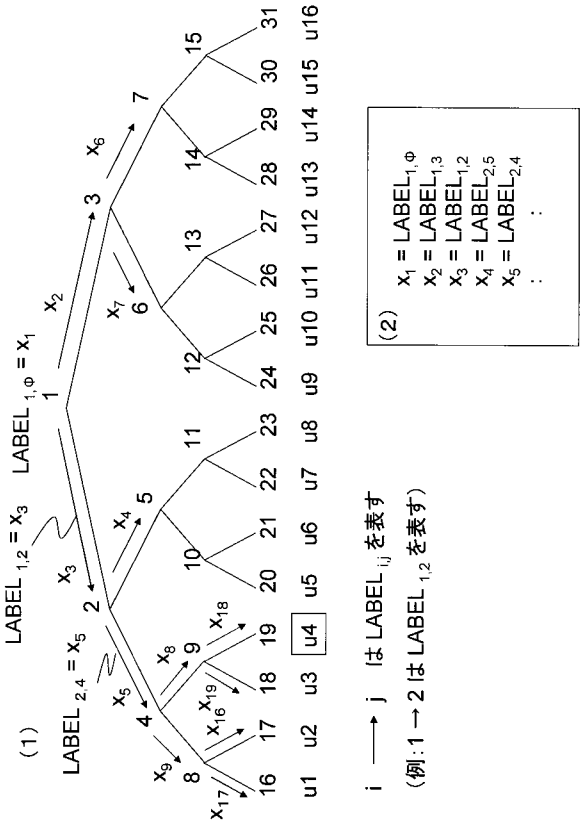
【図１５】



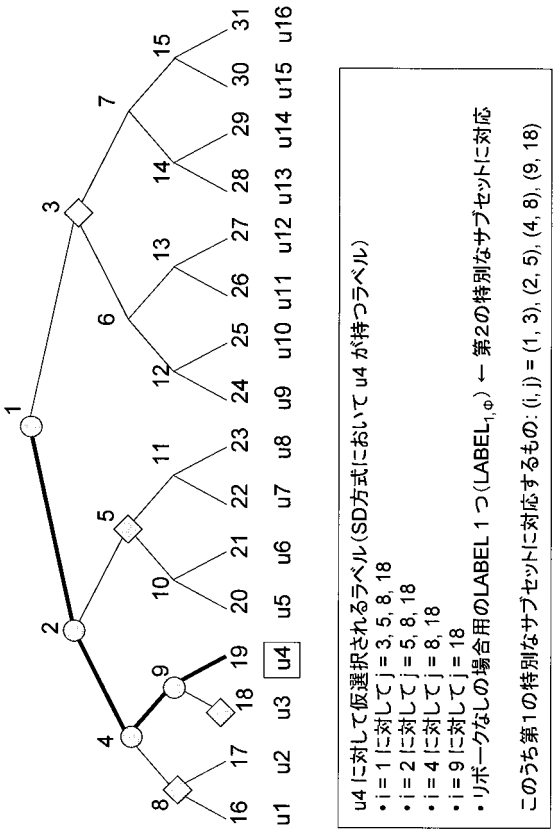
【図１６】



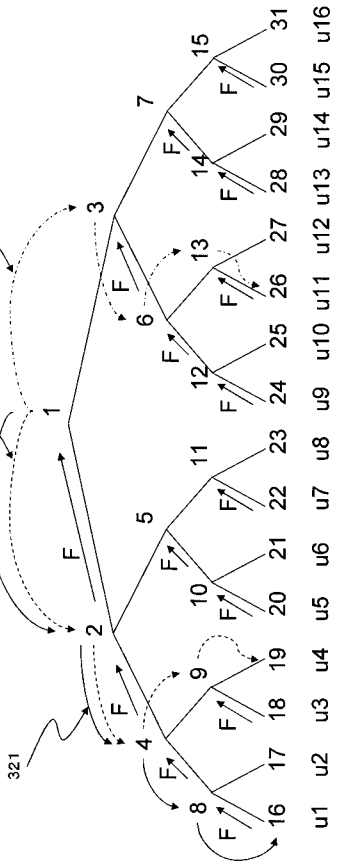
【図１７】



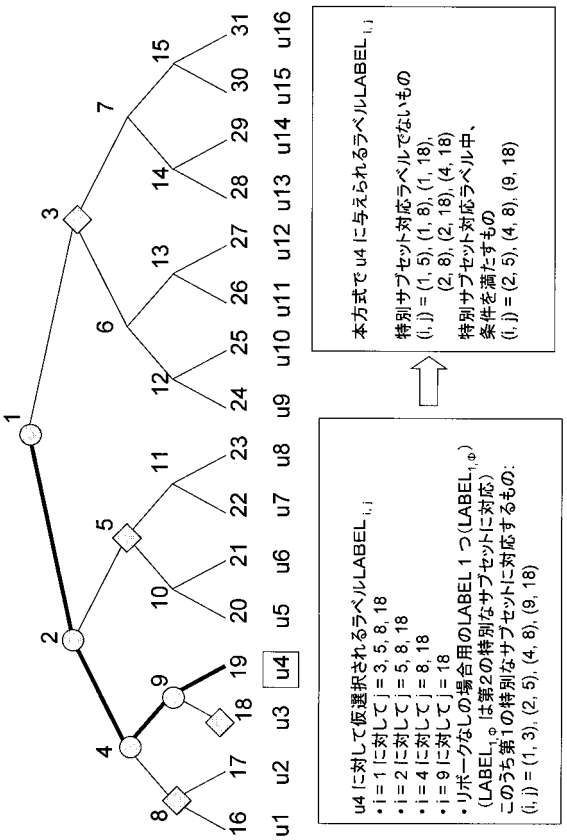
【図１８】



【図１９】



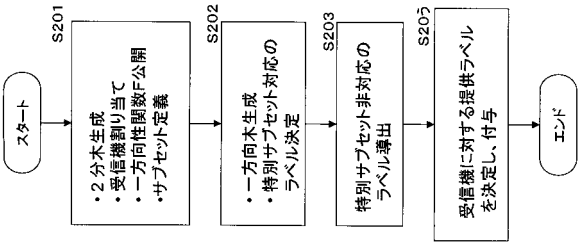
【図２０】



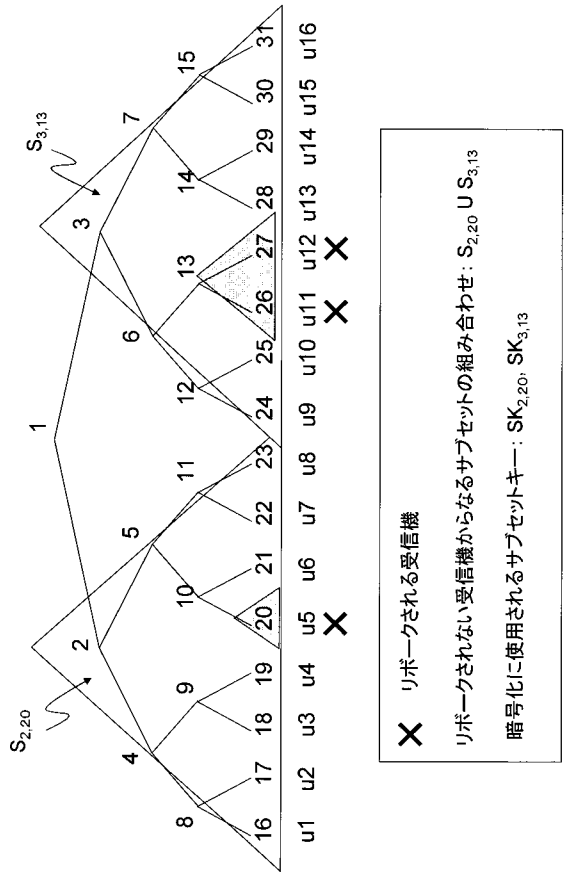
【図２１】

受信機	$path_m$
u1	0000
u2	1000
u3	0100
u4	1100
u5	0010
u6	1010
u7	0110
u8	1110
u9	0001
u10	1001
u11	0101
u12	1101
u13	0011
u14	1011
u15	0111
u16	1111

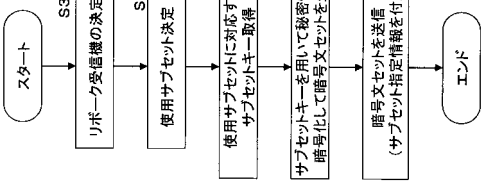
【図２２】



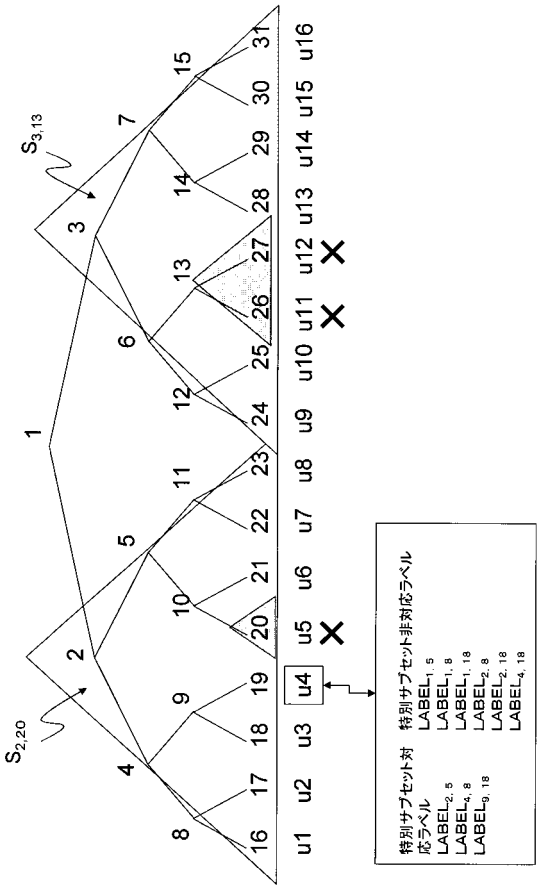
【図２３】



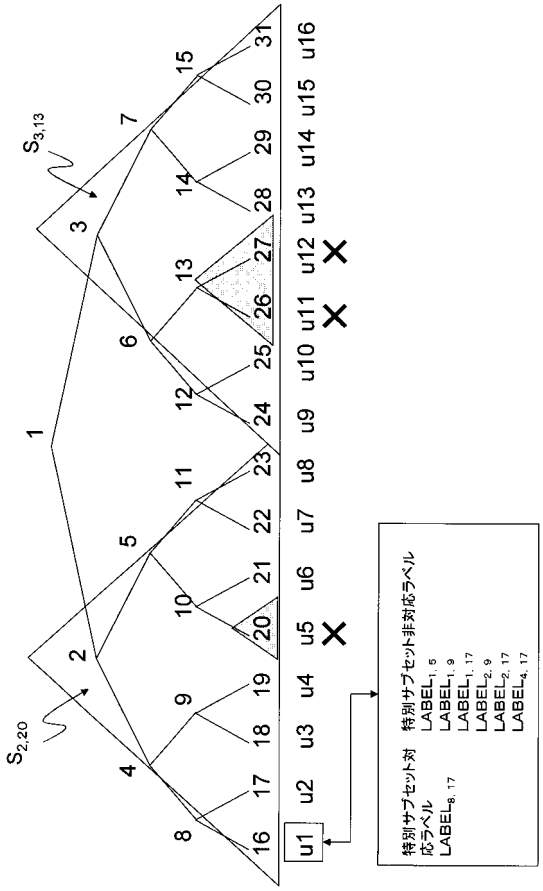
【図２４】



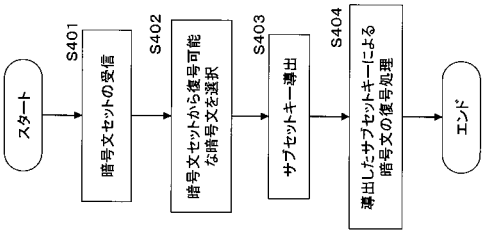
【図２５】



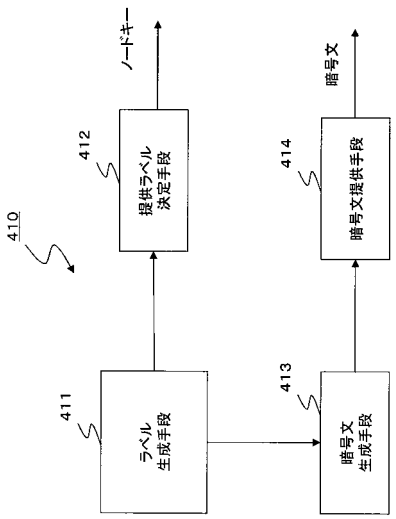
【図２６】



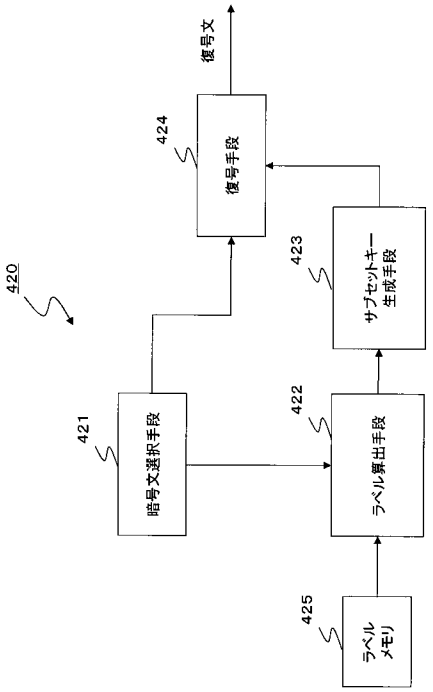
【図２７】



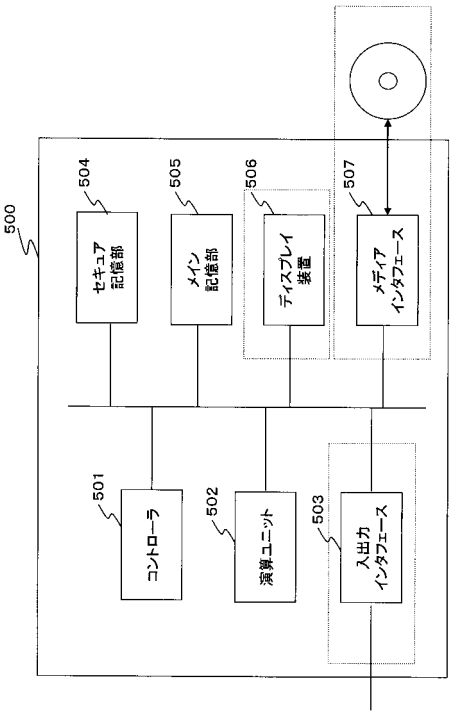
【図２８】



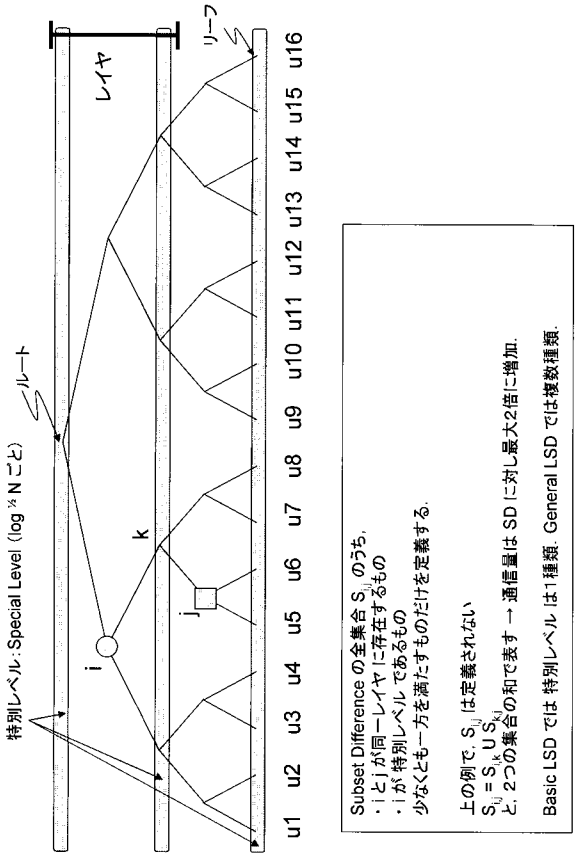
【図２９】



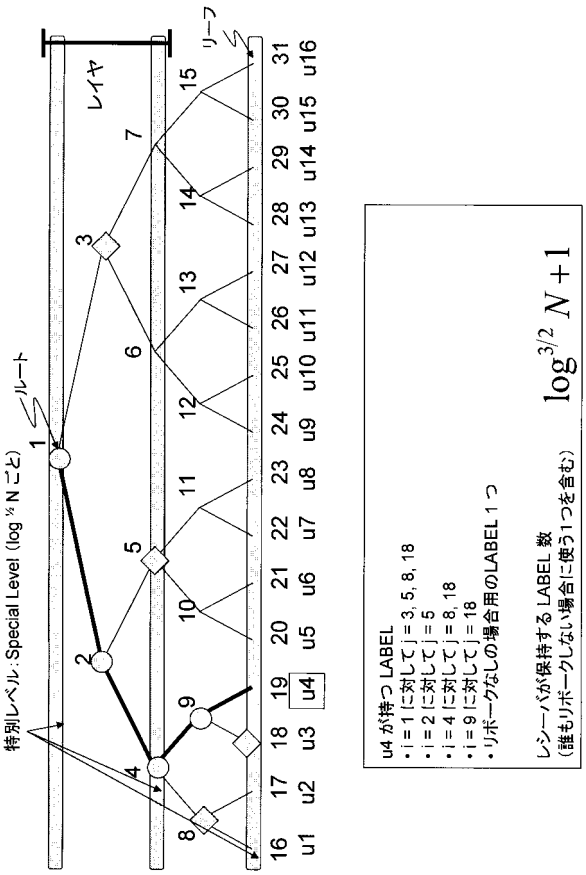
【図３０】



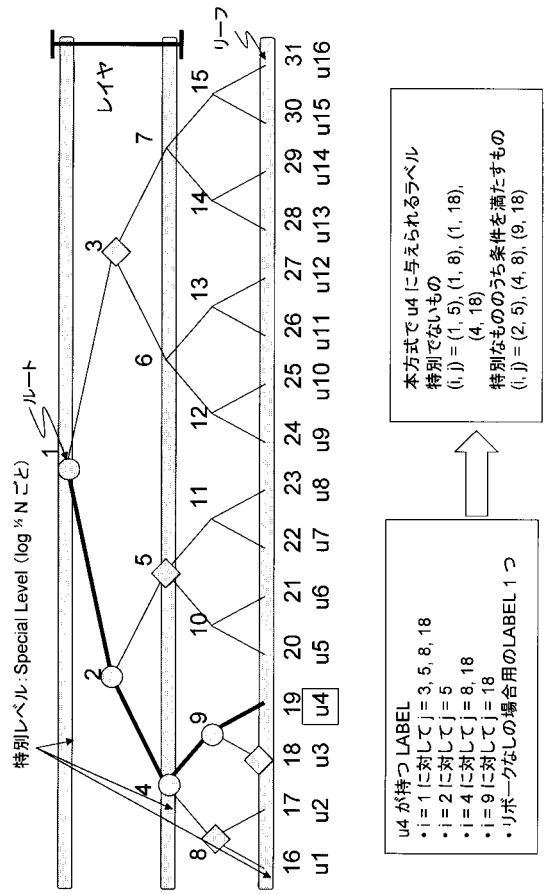
【図３１】



【図３２】



【図３３】


特別レベル：Special Level (log ½ N ごと)
ルート
リーフ
レイヤ
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
• リボーグなしの場合用の LABEL 1 つ
本方式で u4 に与えられるラベル
特別でないもの
(i, j) = (1, 5), (1, 8), (1, 18),
(4, 18)
特別なもののうち条件を満たすもの
(i, j) = (2, 5), (4, 8), (9, 18)

フロントページの続き

(56)参考文献 特開２００１－１４８６９５（ＪＰ，Ａ）
特開平９－２４５０４５（ＪＰ，Ａ）
国際公開第２００２／０６０１１６（WO，Ａ２）
浅野 智之, SD/LSD Boradcast Encryption 方式のラベルの削減手法, 2004年暗号と情報セキュリティシンポジウム予稿集, ２００４年 1月, p.1-6

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８