(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2008 年9 月25 日 (25.09.2008)

PCT

(10) 国際公開番号
WO 2008/114540 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2008/051745

(22) 国際出願日: 2008 年2 月4 日 (04.02.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2007-073172 2007 年3 月20 日 (20.03.2007) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 浅野 智之 (ASANO, Tomoyuki) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 草川 雅文 (KUSAKAWA, Masafumi) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 亀谷 美明, 外(KAMEYA, Yoshiaki et al.); 〒1600004 東京都新宿区四谷３－１－３ 第一冨澤ビル はづき国際特許事務所 四谷オフィス Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

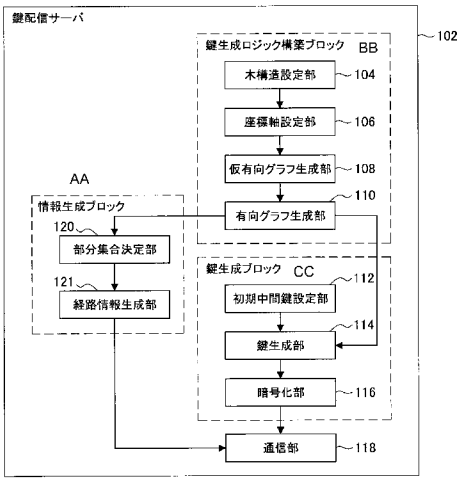
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

[続葉有]

(54) Title: KEY PROVIDING SYSTEM, KEY PROVIDING APPARATUS, TERMINAL APPARATUS, KEY PROVIDING METHOD, AND KEY GENERATING METHOD

(54) 発明の名称: 鍵提供システム、鍵提供装置、端末装置、鍵提供方法、及び鍵生成方法

[図8]



102 KEY DELIVERING SERVER
AA INFORMATION GENERATING BLOCK
120 SUBSET DECIDING PART
121 PATH INFORMATION GENERATING PART
BB KEY GENERATION LOGIC ESTABLISHING BLOCK
104 TREE STRUCTURE SETTING PART
106 COORDINATE AXES SETTING PART
108 TEMPORARY DIRECTED GRAPH GENERATING PART
110 DIRECTED GRAPH GENERATING PART
CC KEY GENERATING BLOCK
112 INITIAL INTERMEDIATE KEY SETTING PART
114 KEY GENERATING PART
116 ENCRYPTING PART
118 COMMUNICATING PART

(57) Abstract: A key providing apparatus capable of providing, to a predetermined terminal apparatus, a key for use in encrypting or decrypting data. The key providing apparatus comprises an acquiring part that acquires a directed graph formed such that at least one directed branch connects coordinate points in a coordinate system including a plurality of coordinate points with which subsets representative of combinations of terminal apparatuses are associated; an extracting part that extracts information of all of the directed branches included in a directed path connecting the starting point of the directed graph and a predetermined coordinate point; and a key generating part that generates, based on the directed graph, a key associated with a subset to which a predetermined terminal apparatus belongs. The key providing apparatus provides the information of the directed branches to the predetermined terminal apparatus.

(57) 要約: データの暗号化又は復号に用いる鍵を所定の端末装置に提供することが可能な鍵提供装置が提供される。当該鍵提供装置は、複数の端末装置の組合せを表す部分集合が各々に対応付けられた複数の座標点を有する座標軸上に、座標点間を結ぶ少なくとも１つの有向枝を配置して形成された有向グラフを取得する取得部と、有向グラフの始点と所定の座標点とを結ぶ有向パスに含まれる全ての有向枝の情報を抽出する抽出部と、有向グラフに基づき、所定の端末装置が所属する部分集合に対応付けられた鍵を生成する鍵生成部と、を備え、有向枝の情報を所定の端末装置に提供する。

WO 2008/114540 A1

KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

鍵提供システム、鍵提供装置、端末装置、鍵提供方法、及び鍵生成方法

技術分野

[0001] 本発明は、鍵提供システム、鍵提供装置、端末装置、鍵提供方法、及び鍵生成方法に関する。

背景技術

[0002] 近年、パーソナルコンピュータ(以下、PC)、携帯電話、及びデジタル家電等の情報機器が一般にも広く普及してきている。また、これらの情報機器やそれらの間を繋ぐ情報通信に関する技術が非常に大きく発達してきており、これらの情報機器を利用した音楽配信や映像配信といったコンテンツ配信サービスが広く展開されるようになってきている。例えば、CATV(Community Antenna TeleVision)、衛星放送、又はインターネット等を利用した有料放送、CD(Compact Disc)又はDVD(Digital Versatile Disc)等物理メディアを利用したコンテンツ販売等がコンテンツ配信サービスの一例である。

[0003] しかし、このようなコンテンツ配信サービスを提供するには、当該サービスの提供者(以下、システム管理者)と視聴者との間で締結した契約に基づき、その契約者のみがコンテンツを取得できるようにする仕組みが必要とされる。この問題に対し、例えば、システム管理者が契約者に対して所定の鍵を提供しておき、暗号化されたコンテンツMと共に、コンテンツMを暗号化するために利用したコンテンツ鍵mekを前記所定の鍵により生成するためのヘッダ情報hとを配信する仕組みが考案されている。

[0004] 上記の仕組みを実現させる具体的な一手段として、ブロードキャスト・エンクリプション(Broadcast Encryption)方式と呼ばれるコンテンツ配信方式が知られている。このブロードキャスト・エンクリプション方式とは、各契約者を集合の要素に対応付けた上で、契約者全体を表す契約者集合を複数の部分集合に分割し、特定の部分集合に属する契約者のみがコンテンツ鍵mekを取得できるようなヘッダhを配信する方式である。つまり、当該方式を適用すると、システム管理者が指定した特定の契約者を排除してコンテンツMの配信を実現することができる。しかし、現実的には、システ

ム管理者側のサーバ装置(以下、センタ)及び契約者側の端末装置におけるコンテンツ鍵mekの生成に係る演算負荷、及びサーバ装置と端末装置との間の通信負荷等を考慮すると、従来のブロードキャスト・エンクリプション方式をより効率化する必要がある。

[0005] 具体的には、上記のコンテンツ配信をする際に、センタが配信するヘッダhのサイズに応じて増大する通信量、各端末装置が保持すべき鍵数に応じて増大するメモリ量、及び各端末装置がコンテンツ鍵mekを生成するために必要な計算量を如何にして低減させるかということが問題となる。上記の各量は、契約者集合の分割方法によって大きく異なる。そこで、効率的なコンテンツ配信を実現させるため、契約者集合の分割方法に工夫を凝らした種々のブロードキャスト・エンクリプション方式が提案されている。例えば、下記の非特許文献1には、上記の各量を低減させるための一つの手段として、Nuttapong Attrapadung and Hideki Imaiらにより、Subset Incremental Chain Based Broadcast Encryption方式と呼ばれるコンテンツ配信方式が開示されている(以下、AI05方式)。

[0006] 非特許文献1:Nuttapong Attrapadung and Hideki Imai、"Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext"、The 28th Symposium on Information Theory and Its Applications(SITA2005)

発明の開示

発明が解決しようとする課題

[0007] また、本件出願人は、上記の非特許文献1に記載のコンテンツ配信方式よりも、各端末装置が鍵を保持するために要求されるメモリ量を低減することが可能な第1の改良方式(以下、A06(A)方式)、各端末装置がコンテンツ鍵を生成するために要求される計算量を低減することが可能な第2の改良方式(以下、A06(B)方式)、及び上記のメモリ量と計算量とを低減させることが可能な第3の改良方式(以下、A06(A+B)方式)を開発し、既に日本国特許庁に特許出願している(A06(A)方式:特願2006-310182、A06(B)方式:特願2006-310213、A06(A+B)方式:特願2006-310226)。当該各方式の特徴は、擬似乱数生成器を利用してコンテンツ鍵mek

を生成する際に、各方式固有の有向グラフにより表現される鍵生成アルゴリズムに基づき、擬似乱数生成演算を実行する点にある。

[0008] しかし、上記の各方式に限らず、ある方式に従って一つの部分集合に対応する鍵から他の部分集合に対応する鍵を生成する場合、例えば、複数の鍵生成経路の情報を含む有向グラフのような集合関係情報を端末装置側で全て保持しなければならないとすると、複数の鍵生成経路の情報を保持するために要する記憶容量が大きくなってしまうという問題がある。一方、鍵提供装置が有する複数の鍵生成経路の情報を端末装置が全て取得しなければならないとすると、複数の鍵生成経路の情報を端末装置が取得するために伝播される容量が大きくなってしまうという問題もある。

[0009] 本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、端末装置が予め全ての鍵生成経路情報を伝播又は保持している場合に比べて、端末装置が鍵生成に要する情報を伝播又は保持するために必要な容量を低減することが可能な、新規かつ改良された鍵提供システム、鍵提供装置、端末装置、鍵提供方法及び鍵生成方法を提供することにある。

課題を解決するための手段

[0010] 上記課題を解決するために、本発明のある観点によれば、複数の端末装置と、これら複数の端末装置に情報の暗号化又は復号に用いる鍵情報を提供する鍵提供装置とを備える鍵提供システムが提供される。

また、前記鍵提供装置は、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を取得する集合関係情報取得部と、前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出部と、この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供部と、を備えていてもよい。

さらに、前記端末装置は、前記一部の鍵生成経路情報を取得する鍵生成経路情報取得部と、前記一部の鍵生成経路情報に基づき、前記複数の集合情報の一つに

対応する鍵情報から前記複数の集合情報の他の一つに対応する鍵情報を生成する鍵情報生成部と、を備えていてもよい。

[0011] また、上記課題を解決するために、本発明の別の観点によれば、複数の端末装置に対してデータの暗号化又は復号に用いる鍵情報を提供する鍵提供装置が提供される。当該鍵提供装置は、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を取得する集合関係情報取得部と、前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出部と、この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供部と、を備えることを特徴とする。

[0012] また、前記鍵生成経路情報提供部は、ネットワークを介して前記鍵生成経路情報を前記端末装置に送信する通信部を備えていてもよい。

[0013] また、前記鍵生成経路情報提供部は、前記鍵生成経路情報を前記端末装置に提供するための記録媒体に記録する記録部を備えていてもよい。

[0014] また、前記複数の集合情報の一つに対応する鍵情報を用いて情報を暗号化する暗号化部と、暗号化された前記情報を前記端末装置に提供する暗号情報提供部と、をさらに備えていてもよい。

[0015] また、前記鍵生成経路情報取得部は、前記集合関係情報として、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報に対応付けられた複数の座標点に対し、当該座標点間を結ぶ有向枝によって形成された有向グラフを取得するように構成されていてもよい。

[0016] また、前記鍵生成経路情報抽出部は、前記一部の鍵生成経路情報として、前記端末装置が属する前記集合情報に対応付けられた座標点に到達する前記有向グラフの一部を抽出するように構成されていてもよい。

[0017] また、前記鍵生成経路情報抽出部は、前記一部の鍵生成経路情報として前記有向グラフの一部を構成する有向枝の終端位置を示す情報を抽出するように構成され

ていてもよい。

[0018] また、前記鍵生成経路情報抽出部は、前記一部の鍵生成経路情報として、前記有向グラフの一部を構成する有向枝の長さを示す情報を抽出するように構成されていてもよい。

[0019] また、前記座標点S_0に対応する前記鍵情報$k(S_0)$の入力に応じて、前記座標点S_0を始端とする全ての前記有向枝の終端の座標点S_1, ・・・, S_mに対応する前記鍵情報$k(S_1)$, ・・・, $k(S_m)$を生成する鍵情報生成部をさらに備えていてもよい。

[0020] また、前記鍵情報は、情報を暗号化又は復号するためのセット鍵kと、当該セット鍵kを生成するための中間鍵tとにより構成されていてもよい。さらに、前記座標点S_0に対応する前記中間鍵$t(S_0)$の入力に応じて、前記座標点S_0に対応する前記セット鍵$k(S_0)$と、前記座標点S_0を始端とする全ての前記有向枝の終端の座標点S_1, ・・・, S_mに対応する前記中間鍵$t(S_1)$, ・・・, $t(S_m)$とを生成する鍵情報生成部をさらに備えていてもよい。

[0021] また、上記課題を解決するために、本発明の別の観点によれば、複数の端末装置に対してデータの暗号化又は復号に用いる鍵情報を提供する鍵提供装置が提供される。当該鍵提供装置は、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を生成する集合関係情報生成部と、前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出部と、この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供部と、を備えることを特徴とする。

[0022] また、上記課題を解決するために、本発明の別の観点によれば、情報の暗号化又は復号に用いる鍵情報を生成する端末装置が提供される。当該端末装置は、複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報の中から抽出さ

れた、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を取得する鍵生成経路情報取得部と、前記一部の鍵生成経路情報に基づき、前記複数の集合情報の一つに対応する鍵情報から前記複数の集合情報の他の一つに対応する鍵情報を生成する鍵情報生成部と、を備えることを特徴とする。

[0023] また、前記鍵生成経路情報取得部は、ネットワークを介して前記鍵生成経路情報を受信する通信部を備えていてもよい。

[0024] また、前記鍵生成経路情報取得部は、前記鍵生成経路情報が記録された記録媒体を取得し、前記記録媒体から前記鍵生成経路情報を読み出す読出部を備えていてもよい。

[0025] また、前記複数の集合情報の他の一つに対応する鍵情報を用いて暗号化された情報を取得する暗号情報取得部と、前記鍵情報生成部により生成された前記複数の集合情報の他の一つに対応する鍵情報を用いて、前記暗号化された情報を復号する復号部と、をさらに備えていてもよい。

[0026] また、前記鍵生成経路情報取得部は、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報に対応付けられた複数の座標点に対し、当該座標点間を結ぶ有向枝によって形成された有向グラフの中から抽出された、前記端末装置が属する前記集合情報に対応付けられた座標点に到達する前記有向グラフの一部を前記一部の鍵生成経路情報として取得するように構成されていてもよい。

[0027] また、前記鍵生成経路情報取得部は、前記一部の鍵生成経路情報として前記有向グラフの一部を構成する有向枝の終端位置を示す情報を取得するように構成されていてもよい。

[0028] また、前記鍵生成経路情報取得部は、前記一部の鍵生成経路情報として、前記有向グラフの一部を構成する有向枝の長さを示す情報を取得するように構成されていてもよい。

[0029] また、前記有向枝の始端S_0に対応する前記鍵情報$k(S_0)$の入力に応じて、前記有向枝の終端の座標点S_1に対応する前記鍵情報$k(S_1)$を生成する鍵情報生成部をさらに備えていてもよい。

[0030] また、前記鍵情報は、情報を暗号化又は復号するためのセット鍵kと、当該セット鍵

kを生成するための中間鍵tとにより構成されていてもよい。さらに、前記有向枝の始端S_0に対応する前記中間鍵t(S_0)の入力に応じて、前記有向枝の始端S_0に対応する前記セット鍵k(S_0)と、前記有向枝の終端S_1に対応する前記中間鍵t(S_1)とを生成する鍵情報生成部をさらに備えていてもよい。

[0031] また、上記課題を解決するために、本発明の別の観点によれば、複数の端末装置に対してデータの暗号化又は復号に用いる鍵情報を提供するための鍵提供方法が提供される。当該鍵提供方法は、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を取得する集合関係情報取得ステップと、前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出ステップと、この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供ステップと、を含むことを特徴とする。

[0032] また、上記課題を解決するために、本発明の別の観点によれば、情報の暗号化又は復号に用いる鍵情報を生成するための鍵生成方法が提供される。当該鍵生成方法は、複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報の中から抽出された、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を取得する鍵生成経路情報取得ステップと、前記一部の鍵生成経路情報に基づき、前記複数の集合情報の一つに対応する鍵情報から前記複数の集合情報の他の一つに対応する鍵情報を生成する鍵情報生成ステップと、を含むことを特徴とする。

[0033] 上記の各構成によると、鍵提供装置により抽出された一部の鍵生成経路情報が端末装置に提供され、端末装置が一つの集合に対応する鍵から他の集合に対応する鍵を導出できるため、鍵提供装置が持つ全ての鍵生成経路情報の提供を受ける場合に比べて、鍵提供装置から端末装置に鍵生成経路情報を伝播するために必要な容量を制限することができる。また、端末装置が予め全ての鍵生成経路情報を保持

している場合に比べても、端末装置が保持のために要する容量を制限することができる。

発明の効果

[0034] 以上説明したように、本発明によれば、端末装置が予め全ての鍵生成経路情報を伝播又は保持する場合に比べて、端末装置が鍵生成に要する情報を伝播又は保持するために必要な容量を低減することが可能になる。

図面の簡単な説明

[0035] [図1]本発明の第1及び第2実施形態に係る鍵提供システム100の構成を示す説明図である。

[図2]同実施形態に係る鍵配信サーバ102及び端末装置122のハードウェア構成を示す説明図である。

[図3]同実施形態に係る論理二分木の構造を示す説明図である。

[図4]AI05方式の有向グラフHを示す説明図である。

[図5]AI05方式に係る鍵配信処理の流れを示す説明図である。

[図6]AI05方式に係る鍵配信処理の流れを示す説明図である。

[図7]同実施形態に係る暗号文の復号処理の流れを示す説明図である。

[図8]同実施形態に係る鍵配信サーバ102の機能構成を示す説明図である。

[図9]A06(A+B)方式に係る仮有向グラフI'を生成する処理の流れを示す説明図である。

[図10]A06(A+B)方式の仮有向グラフI'を示す説明図である。

[図11]A06(A+B)方式に係る有向グラフIを生成する処理の流れを示す説明図である。

[図12]A06(A+B)方式に係る有向グラフIを生成する処理の流れを示す説明図である。

[図13]A06(A+B)方式に係る有向グラフIを生成する処理の流れを示す説明図である。

[図14]A06(A+B)方式に係る有向グラフIを生成する処理の流れを示す説明図である。

[図15]A06(A+B)方式の有向グラフIを示す説明図である。

[図16]AI05方式の有向グラフHに同実施形態を適用する際に参照される有向パスの一例を示す説明図である。

[図17]AI05方式の有向グラフHに同実施形態を適用する際に参照される有向パスの一例を示す説明図である。

[図18]A06(A+B)方式の有向グラフIに同実施形態を適用する際に参照される有向パスの一例を示す説明図である。

[図19]同実施形態に係る端末装置122の機能構成を示す説明図である。

[図20]本発明の第1実施形態に係る鍵生成処理の流れを示す説明図である。

[図21]本発明の第2実施形態に係る鍵生成処理の流れを示す説明図である。

[図22]本発明の第1及び第2実施形態の応用例である放送暗号化システム300の構成を示す説明図である。

[図23]本発明の第1及び第2実施形態の応用例である放送暗号化システム400の構成を示す説明図である。

符号の説明

[0036]
100 鍵提供システム
102 鍵配信サーバ
104 木構造設定部
106 座標軸設定部
108 仮有向グラフ生成部
110 有向グラフ生成部
112 初期中間鍵設定部
114 鍵生成部
116 暗号化部
118 通信部
120 部分集合決定部
121 経路情報生成部
122 端末装置

124 通信部

126 判断部

128 鍵生成部

130 復号部

202 コントローラ

204 演算ユニット

206 入出力インターフェース

208 セキュア記憶部

210 メイン記憶部

212 ネットワークインターフェース

216 メディアインターフェース

218 情報メディア

発明を実施するための最良の形態

[0037] 以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0038] ＜第1実施形態＞

以下、本発明の第1実施形態に係る鍵提供システム100の構成、及び鍵配信に係る具体的な方式について詳細に説明する。

[0039] ［概要］

まず、本実施形態に係る鍵提供システム100の構成について詳細に説明するに先立ち、本実施形態に係る鍵配信方式の概要について簡単に説明する。

[0040] 本実施形態は、種々の鍵配信方式に適用することが可能であるが、説明の都合上、本実施形態をAI05方式、及びA06（A＋B）方式に適用するケースを例に挙げて説明する。そこで、本実施形態を適用可能なAI05方式等の基本的な考え方について簡単に説明する。

[0041] AI05方式等では、通常のブロードキャスト・エンクリプション方式と同様、鍵提供システムに含まれる各端末装置を集合の要素に対応付け、端末装置全体の集合を考

える。そして、当該集合を分割して得られる複数の部分集合を利用して鍵配信を実行する。つまり、この部分集合により端末装置の組合せが表現される。まず、鍵配信サーバは、論理二分木(BT;Binary Tree)を形成して各端末装置を葉ノードに対応付ける。次いで、鍵配信サーバは、所定の規則に則って上記の部分集合を要素とする複数の「部分集合の集合」を生成し、当該各部分集合の集合をBTの根ノード、及び各中間ノードに対応付ける。さらに、鍵配信サーバは、上記の部分集合の集合に含まれる複数の部分集合を所定の規則(以下、ジャンプと呼ぶことがある)に基づいて関連付ける。そして、この部分集合間の関係を表すのが有向グラフ又は有向枝である。なお、集合及びその集合の要素である部分集合は、上記の集合情報の一例である。また、AI05方式等により生成される有向グラフは、上記の集合関係情報の一例である。さらに、それを構成する有向枝は、上記の鍵生成経路情報の一例である。但し、上記の鍵生成経路情報は、例えば、1本以上の有向枝により構成される鍵生成経路を表す情報であるか、又は空集合に対応する有向グラフである。

[0042] 上記の有向グラフは、上記の部分集合の集合に含まれる各部分集合が各座標点に対応付けられた座標軸上に形成され、上記のジャンプに基づいて複数の座標点間を連結する有向枝により構成されている。鍵配信サーバは、上記のBTに含まれる根ノード、及び各中間ノードに対応付けられた部分集合の集合毎に、それに含まれる複数の部分集合間の関係が表現された有向グラフを形成する。

[0043] さらに、鍵配信サーバは、配信先となる端末装置が含まれる部分集合を選択し、当該部分集合が含まれる有向グラフを特定する。そして、鍵配信サーバは、特定された有向グラフに基づいて擬似乱数生成器(PRSG;Pseudo－Random Sequence Generator)による演算を繰り返すことによって鍵を生成する。AI05方式の特徴は、従来のブロードキャスト・エンクリプション方式に比べて、通信量、各端末装置が保持すべき鍵数、各端末装置が鍵生成に要する計算量を削減するように、全ての端末装置を表す集合を部分集合に分割する点にある。このように、AI05方式等を適用した鍵配信方式では、有向グラフを利用して各端末装置に配信する鍵を生成することができる。

[0044] なお、A06(A)方式では、有向グラフを構成する有向枝の長さを短くする処理を加

えることにより、上記のAI05方式よりも各端末装置が保持すべき鍵数を低減させる改良が施されている。また、A06(B)方式では、有向枝の長さが長くなるように有向グラフを形成することにより、上記のAI05方式よりも各端末装置が鍵生成に要する計算量を低減させる改良が施されている。さらに、A06(A+B)方式では、A06(B)方式と同様にして有向枝の長い有向グラフを形成した後、A06(A)方式と同様に所定の有向枝を短い有向枝に置換することにより、上記のAI05方式よりも各端末装置が鍵生成に要する計算量及び保持すべき鍵数を低減させる改良が施されている。従って、A06(A)、A06(B)、及びA06(A+B)の各方式を適用することにより、AI05方式よりも端末装置に掛かる負荷を低減させることができる。

[0045] しかし、上記のAI05方式等には、各端末装置が鍵を生成するために必要な有向グラフの情報を如何にして取得するかということについて明確に開示がされておらず、各端末装置が予め有向グラフの情報を全て保持しているか、又は各端末装置が鍵配信サーバと同じアルゴリズムに基づいて各自で有向グラフを生成しているという暗黙の仮定が存在している。しかし、現実的な状況に鑑み、鍵提供システムに含まれる端末装置の数を想定すると、各端末装置が保持すべき有向グラフの情報量、及び有向グラフを生成するための計算量は膨大であるため、一般的な端末装置が有する限られたリソースの中では実現が困難である。

[0046] より具体的に、上記のA06(B)方式の場合で考えてみると、通常、鍵提供システムに含まれる端末装置の数nはn＝2^{32}程度であるため、有向枝1本の情報を4byte程度で表現できたとしても、各端末装置が保持すべき情報量は約32GByteにもなる。また、各端末装置が有向グラフを生成する場合には、端末装置の数n＝2^{32}に対し、(n－1)本の有向枝を算出する必要があるため、各端末装置が有向グラフを生成するのに掛かる演算負荷は非常に大きいと言える。

[0047] しかし、上記の各方式では、各端末装置がコンテンツ鍵mekを生成する際に、予め各端末装置が保持している各有向グラフの情報を利用することが示唆されているのみであり、具体的な手段については示されていなかった。上記の通り、契約者数が多い場合には、各端末装置が保持すべき有向グラフの情報量が膨大になるため、その情報を端末装置に格納しておくのは現実的に困難である。また、各端末装置がそれ

ぞれ有向グラフを算出する場合には、各端末装置の演算量が膨大になり実現が困難である。

[0048] そこで、本実施形態に係る鍵配信サーバは、各端末装置が鍵生成に要する有向グラフの情報を提供する構成を有する。また、各端末装置は、鍵配信サーバから取得した有向グラフの情報に基づいて擬似乱数演算を実行して必要な鍵を生成する構成を有する。

[0049] 以上、本実施形態を適用可能な鍵配信方式について簡単に説明した。もちろん、本実施形態を適用可能な鍵配信方式は、上記のAI05、A06(A)、A06(B)、A06(A+B)の各方式に限定されるものではなく、他の鍵配信方式にも適用することが可能である。以下では、説明の都合上、本実施形態をAI05方式、及びA06(A+B)方式に適用する場合について詳細に説明するが、当業者であれば、当該記載に基づいて容易に他の鍵配信方式への適用手段を想起することが可能である。

[0050] [鍵提供システム100の構成]

ここで、図1を参照しながら、本発明の第1実施形態に係る鍵提供システム100の構成について簡単に説明する。図1は、本実施形態に係る鍵提供システム100の構成を示す説明図である。

[0051] 図1を参照すると、鍵提供システム100は、主に、鍵配信サーバ102と、端末装置122と、ネットワーク10とにより構成される。なお、鍵配信サーバ102は、鍵提供装置の一例である。

[0052] (ネットワーク10)

ネットワーク10は、鍵配信サーバ102と端末装置122とを双方向通信又は一方向通信可能に接続する通信回線網である。ネットワーク10は、例えば、インターネット、電話回線網、衛星通信網、同報通信路等の公衆回線網、WAN(Wide Area Network)、LAN(Local Area Network)、IP-VPN(Internet Protocol-Virtual Private Network)、ワイヤレスLAN等の専用回線網等により構成されており有線/無線を問わない。

[0053] (鍵配信サーバ102)

鍵配信サーバ102は、コンテンツ配信時に種々の電子データを暗号化して配信す

ることが可能である。例えば、鍵配信サーバ102は、コンテンツを暗号化又は復号するためのコンテンツ鍵を生成して配信することが可能である。なお、コンテンツ鍵は、例えば、擬似乱数生成器により算出された乱数(擬似乱数)、所定の文字列、又は数列等により表現されていてもよい。さらに、コンテンツ鍵は、暗号化用のコンテンツ鍵と復号用のコンテンツ鍵とにより構成されていてもよい。そして、鍵配信サーバ102は、このコンテンツ鍵を用いて、所定の暗号化ロジックに基づきコンテンツを暗号化することができる。さらに、鍵配信サーバ102は、コンテンツ及びコンテンツ鍵の一方又は両方を任意の端末装置122に対して配信することが可能である。

[0054] さらに、鍵配信サーバ102は、コンテンツ鍵を暗号化又は復号するための複数のセット鍵を生成することが可能である。このとき、鍵配信サーバ102は、擬似乱数生成器を利用し、所定の有向グラフに基づいて複数のセット鍵を生成する。また、鍵配信サーバ102は、各セット鍵を用いてコンテンツ鍵を暗号化し、この暗号化されたコンテンツ鍵を所定の端末装置122に対して配信する。さらに、鍵配信サーバ102は、所定のセット鍵を生成するために利用した有向グラフの情報を所定の端末装置122に対して配信することも可能である。なお、セット鍵は、上記の鍵情報の一例である。また、コンテンツ鍵は、上記の鍵情報により暗号化／復号される情報の一例である。

[0055] 上記の複数のセット鍵は、それぞれ、多数の契約者の中から選択された複数の契約者の部分集合群に対応付けされており、鍵配信サーバ102は、コンテンツの再生を許諾する契約者(以下、許諾契約者)の集合だけがコンテンツ鍵を復号できるようにセット鍵を生成し、それを用いてコンテンツ鍵を暗号化し、全ての契約者の端末装置122に対して暗号化されたコンテンツ鍵を配信する。このように、鍵配信サーバ102は、コンテンツだけでなく、コンテンツ鍵も暗号化して配信するように構成される。もちろん、コンテンツを暗号化して配信することにより、ある程度のセキュリティレベルを確保することができるけれども、多数の契約者の中からコンテンツの使用が許諾される契約者を追加又は削除する際にフレキシブルに対応するためにはコンテンツ鍵を暗号化して配信する方が有利である。

[0056] 上記の構成により、所定の端末装置122にのみ暗号化されたコンテンツ鍵を復号することが可能になるため、所定の端末装置122だけがコンテンツを復号して視聴す

ることができるようになる。もし、許諾契約者の集合が変更された場合には、鍵配信サーバ102は、コンテンツ鍵の暗号化に用いるセット鍵を変更することにより対応可能である。

[0057] なお、上記の擬似乱数生成器は、所定のシード値を入力することによって長周期の擬似的な乱数列を出力することが可能な装置又はプログラムであり、線形合同法やメルセンヌ・ツイスター法等のロジックを用いて実現されるものである。もちろん、本実施形態に適用可能な擬似乱数生成器は、これに限定されるものではなく、他のロジックを用いて擬似乱数を発生させてもよいし、或いは、特殊な情報又は条件を含んだ擬似乱数列を生成することが可能な装置又はプログラムであってもよい。

[0058] なお、鍵配信サーバ102は、サーバ機能を備えたパーソナルコンピュータ(PC;Personal Computer)等の情報処理装置により構成され、ネットワーク10を介して各種の情報を外部装置に送信可能である。例えば、鍵配信サーバ102は、ブロードキャスト・エンクリプション方式の暗号鍵を生成して、この暗号鍵を端末装置122に配信することができる。また、鍵配信サーバ102は、例えば、映像配信サービス、又は電子音楽配信サービス等のコンテンツ配信サービスを提供するコンテンツ配信サーバとしての機能を具備していてもよく、端末装置122に対してコンテンツを配信することが可能な機能を有していてもよい。なお、鍵配信サーバ102とコンテンツ配信サーバとを別装置として構成することも勿論可能である。

[0059] ここで、コンテンツとは、例えば、映画、テレビジョン番組、ビデオプログラム、図表等の動画又は静止画からなる映像(Video)コンテンツ、音楽、講演、ラジオ番組等の音声(Audio)コンテンツ、ゲームコンテンツ、文書コンテンツ、又はソフトウェア等が含まれる任意のコンテンツデータであってもよい。また、映像コンテンツとは、映像データのみならず、音声データを含んでいてもよい。

[0060] (端末装置122)

端末装置122は、鍵配信サーバ102から種々の情報を受信することができる。例えば、端末装置122は、鍵配信サーバ102により配信されたコンテンツ又はコンテンツ鍵を受信することができる。また、端末装置122は、鍵配信サーバ102から受信したコンテンツ鍵を用いて、暗号化されたコンテンツを復号することができる。ただし、鍵

配信サーバ102から送信されるコンテンツ又はコンテンツ鍵は、所定のセット鍵により暗号化されているため、当該コンテンツ又はコンテンツ鍵を復号しなくてはならない。そこで、端末装置122は、鍵配信サーバ102から取得した所定のセット鍵を利用して暗号化されたコンテンツ又はコンテンツ鍵を復号することができる。さらに、端末装置122は、予め保持しているセット鍵又は所定のセット鍵を生成可能な中間鍵を利用して、鍵配信サーバ102がコンテンツ又はコンテンツ鍵を暗号化する際に用いたセット鍵を生成することができる。このとき、端末装置122は、鍵配信サーバ102から取得した有向グラフに関する情報に基づいて、自己が保持するセット鍵又は中間鍵を擬似乱数生成器に入力して所望のセット鍵を生成することができる。なお、中間鍵は、上記の鍵情報の一例である。

[0061] 上記の構成により、端末装置122は、所望のセット鍵を生成するために必要な有向グラフを生成する必要がなくなり、保持すべき情報量を低減させることが可能な上、セット鍵の生成に掛かる演算負荷を低減させることが可能になる。

[0062] なお、端末装置122は、ネットワーク10を介して外部装置とデータ通信が可能な端末装置であり、各契約者によって所有される。端末装置122は、例えば、図示のようにパーソナルコンピュータ等の情報処理装置により構成されるが、かかる例に限定されず、ネットワーク10を介して情報通信が可能な通信機能を有する機器であれば、例えば、PDA(Personal Digital Assistant)、家庭用ゲーム機、DVD／HDDレコーダ、又はテレビジョン受像器等の情報家電、テレビジョン放送用のチューナやデコーダ等により構成することも可能である。また、端末装置122は、例えば、携帯型ゲーム機、携帯電話、携帯型映像／音声プレーヤ、PDA、又はPHS等の契約者が持ち運び可能な携帯端末(Portable Device)であってもよい。

[0063] 以上、本実施形態に係る鍵提供システム100の構成について簡単に説明した。次に、鍵提供システム100を構成する鍵配信サーバ102及び端末装置122のハードウェア構成の具体例について簡単に説明する。

[0064] [鍵配信サーバ102及び端末装置122のハードウェア構成]

ここで、図2を参照しながら、本実施形態に係る鍵配信サーバ102及び端末装置122のハードウェア構成について簡単に説明する。図2は、本実施形態に係る鍵配信

サーバ102又は端末装置122の機能を実現可能なハードウェア構成の一例である。

[0065] 図2を参照すると、鍵配信サーバ102及び端末装置122は、例えば、コントローラ202と、演算ユニット204と、入出力インターフェース206と、セキュア記憶部208と、メイン記憶部210と、ネットワークインターフェース212と、メディアインターフェース216とにより構成される。

[0066] (コントローラ202)

コントローラ202は、バスを介して他の構成要素に接続されており、主に、メイン記憶部210に格納されたプログラム及びデータに基づいて装置内の各部を制御する役割を担う。なお、コントローラ202は、CPU(Central Processing Unit)等の演算処理装置により構成されていてもよい。

[0067] (演算ユニット204(鍵配信サーバ102の場合))

鍵配信サーバ102が備える演算ユニット204は、例えば、コンテンツの暗号化、コンテンツ鍵の暗号化、有向グラフの生成、セット鍵の生成、及びセット鍵を生成するために用いる中間鍵の導出を実行することができる。従って、演算ユニット204は、所定のデータ(シード値等)に基づいて擬似乱数を発生させる擬似乱数生成器として機能し得ると同時に、所定のアルゴリズムに基づいてコンテンツ又はコンテンツ鍵を暗号化することが可能である。なお、上記所定のアルゴリズムは、演算ユニット204が判読可能なプログラムとしてメイン記憶部210に格納されていてもよい。また、上記所定のデータは、メイン記憶部210又はセキュア記憶部208に格納されていてもよい。なお、演算ユニット204は、上記の各種演算処理を実行して得られた出力結果をメイン記憶部210又はセキュア記憶部208に記録することができる。また、演算ユニット204は、CPU等の演算処理装置により構成される。なお、演算ユニット204は、上記のコントローラ202と一体に形成されていてもよい。

[0068] (演算ユニット204(端末装置122の場合))

端末装置122が備える演算ユニット204は、例えば、コンテンツの復号、コンテンツ鍵の復号、セット鍵の生成、及びセット鍵を生成するために用いる中間鍵の生成を実行することができる。従って、演算ユニット204は、所定のデータ(シード値等)に基づいて擬似乱数を発生させる擬似乱数生成器として機能し得ると同時に、所定のアル

ゴリズムに基づいてコンテンツ又はコンテンツ鍵を復号することが可能である。なお、所定のアルゴリズムは、演算ユニット204が判読可能なプログラムとしてメイン記憶部210に格納されていてもよい。また、所定のデータは、メイン記憶部210又はセキュア記憶部208に格納されていてもよい。なお、演算ユニット204は、上記の各種演算処理を実行して得られた出力結果をメイン記憶部210又はセキュア記憶部208に記録することが可能である。また、演算ユニット204は、例えば、CPU等の演算処理装置により構成される。なお、演算ユニット204は、上記のコントローラ202と一体に形成されていてもよい。

[0069] （入出力インターフェース206）

入出力インターフェース206は、主に、ユーザがデータを入力するための入力デバイスと、演算結果又はコンテンツの中身を出力する出力デバイスとに接続されている。例えば、入力デバイスは、キーボード、マウス、トラックボール、タッチペン、キーパッド、又はタッチパネル等であってもよい。これらの入力デバイスは、入出力インターフェース206に対して有線又は無線により接続されていてもよい。また、入力デバイスは、有線又は無線により接続された携帯電話やPDA等の携帯型電子機器であってもよい。一方、出力デバイスは、例えば、ディスプレイ等の表示装置、又はスピーカ等の音声出力デバイス等であってもよい。そして、出力デバイスは、入出力インターフェース206に対して有線又は無線により接続されていてもよい。なお、上記の入出力デバイスは、鍵配信サーバ102又は端末装置122に対して一体として形成されていてもよい。

[0070] なお、入出力インターフェース206は、バスを介して他の構成要素に接続されており、入出力インターフェース206を介して入力されたデータをメイン記憶部210等に伝達することが可能である。逆に、入出力インターフェース206は、メイン記憶部210等に格納されたデータ、ネットワークインターフェース212等を介して入力されたデータ、又は演算ユニット204により当該データに基づき演算して得られた結果等を出力デバイスに出力することができる。

[0071] （セキュア記憶部208）

セキュア記憶部208は、主に、コンテンツ鍵、セット鍵、及び中間鍵等の秘匿が必

要なデータを安全に格納するための記憶装置である。セキュア記憶部208は、例えば、ハードディスク等の磁気記憶装置、光ディスク等の光記憶装置、光磁気記憶装置、又は半導体記憶装置等により構成されていてもよい。また、セキュア記憶部208は、例えば、耐タンパ性を有する記憶装置により構成されていてもよい。

[0072] （メイン記憶部210）

メイン記憶部210は、例えば、コンテンツ又はコンテンツ鍵等を暗号化するための暗号化プログラム、暗号化されたコンテンツ又はコンテンツ鍵等を復号するための復号プログラム、又はセット鍵や中間鍵を生成するための鍵生成プログラム等が格納されていてもよい。また、メイン記憶部210は、演算ユニット204から出力された計算結果を一時的又は永続的に格納したり、入出力インターフェース206、ネットワークインターフェース212、又はメディアインターフェース216等から入力されたデータを格納してもよい。メイン記憶部210は、例えば、ハードディスク等の磁気記憶装置、光ディスク等の光記憶装置、光磁気記憶装置、又は半導体記憶装置等により構成されていてもよい。

[0073] （ネットワークインターフェース212）

ネットワークインターフェース212は、ネットワーク10を介して他の通信装置等に接続されており、例えば、暗号化されたコンテンツ又はコンテンツ鍵、セット鍵、中間鍵等のデータ、暗号化に用いるパラメータ情報、及び許諾契約者の集合に関するデータを送受信するためのインターフェース手段である。ネットワークインターフェース212は、バスを介して他の構成要素に接続されており、ネットワーク10上にある外部装置から受信したデータを他の構成要素に伝達し、又は他の構成要素が有するデータをネットワーク10上にある外部装置に送信することが可能である。

[0074] （メディアインターフェース216）

メディアインターフェース216は、情報メディア218を着脱してデータを読み書きするためのインターフェースであり、バスを介して他の構成要素に接続されている。このメディアインターフェース216は、例えば、装着された情報メディア218からデータを読み出して他の構成要素に伝達し、又は他の構成要素から供給されたデータを情報メディア218に書き込むことが可能である。情報メディア218は、例えば、光ディスク、

磁気ディスク、半導体メモリ等のポータブル記憶媒体（着脱可能な記憶媒体）であってもよいし、又はネットワーク10を介さずに比較的近距離で有線／無線接続された情報端末の記憶媒体等であってもよい。

[0075] 以上、本実施形態に係る鍵配信サーバ102及び端末装置122の機能を実現可能なハードウェア構成の一例を示した。上記の各構成要素は、汎用的な部材を用いて構成されていてもよいし、各構成要素の機能に特化した専用のハードウェアにより構成されていてもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用するハードウェア構成を変更することが可能である。また、上記のハードウェア構成は、あくまでも一例であり、これに限定されるものでないことは言うまでもない。例えば、コントローラ202と演算ユニット204とを同一の演算装置により構成してもよいし、セキュア記憶部208とメイン記憶部210とを同一の記憶装置により構成してもよい。また、利用形態によっては、メディアインターフェース216、又は入出力インターフェース206等を省略する構成も可能である。

[0076] ［本実施形態を適用可能な鍵配信方式］

次に、本実施形態を適用可能な鍵配信方式の例として、AI05方式とA06（A＋B）方式とについて詳細に説明する。もちろん、本実施形態を適用可能な鍵配信方式がこれに限定されないことは言うまでもなく、当業者であれば、以下の記載から他の鍵配信方式に本実施形態を適用する手段を容易に想起することが可能である。

[0077] （AI05方式）

ここで、本実施形態を適用可能なAI05方式について説明する。AI05方式は、コンテンツが配信される端末装置122の集合を複数の部分集合に分け、各部分集合に対応付けられたセット鍵によってコンテンツ鍵を暗号化して配信する方式である。なお、以下で説明する各処理は、主に、鍵配信サーバ102により実行されるものであるが、端末装置122においても、コンテンツ又はコンテンツ鍵を復号するための鍵を生成するために下記アルゴリズムの少なくとも一部が利用されうる。

[0078] AI05方式では、コンテンツ配信の対象となる端末装置122の集合を複数の部分集合に分けて考える。そこで、図3を参照しながら、AI05方式に係る部分集合の分け方について説明する。もちろん、部分集合の分け方は一通りではないが、AI05方式で

は、二分木構造を用いた部分集合の分け方を採用している。AI05方式では、二分木構造を形成する各結節点(ノード)に対し、ノード間の位置関係を考慮して所定の部分集合を対応付けることにより、所定の組合せを有する端末装置122の部分集合を網羅的に選択する。まず、図3を参照しながら、二分木構造の構築方法について説明する。なお、その説明に用いる表現を下記のように定義する。

[0079] (各種定義)

・全ての端末装置(契約者)の集合N={1, ・・・, n}(nは2のべき乗)

自然数i及びj(但し、i≦j)について、

・[i, j]={i, i+1, ・・・, j}

・(i→i)=(i←i)={{i}}

・(i→j)={{i}, {i, i+1}, ・・・, {i, i+1, ・・・, j}}

={[i, i], [i, i+1], ・・・, [i, j]}

・(i←j)={{j}, {j, j−1}, ・・・, {j, j−1, ・・・, i}}

={[j, j], [j, j−1], ・・・, [j, i]}

[0080] さらに、二分木構造上の末端に位置するノードを葉ノード、頂点に位置するノードを根ノード、根ノードと葉ノードとの間に位置する各ノードを中間ノードと呼ぶことにする。また、各葉ノードは、各端末装置122に対応付けられている。図3の例では、BTの葉ノード数nがn=64の場合が示されている。

[0081] (二分木構造の形成)

まず、葉ノードの数がn(例えば、n=64)となるようにBTを作成する。そして、各葉ノードに対し、左端から右方向に向かって番号1, ・・・, nを対応付ける。つまり、番号1, ・・・, nは、各端末装置122に対応付けられる。次いで、ある中間ノードvに割り当てる部分集合を規定するための指標l_v及びr_vを定義する。さらに、ある中間ノードvの下位に位置する葉ノードのうち、最左にある葉ノードの番号をl_v、最右にある葉ノードの番号をr_vと定義する。なお、中間ノードvは、vを指標とするBT上の中間ノードを示す。

[0082] 次に、BT上の中間ノードを2つの集合に分類する。BT上の中間ノードのうち、親ノードの左側に位置する中間ノードの集合をBT_Lと定義し、親ノードの右側に位置する

中間ノードの集合をBT_Rと定義する。なお、BT上で接続された2つのノード間の位置関係について、上位に位置するノードを親ノードと呼び、下位に位置するノードを子ノードと呼ぶことにする。

[0083] （根ノードに対する集合の対応付け）

次に、BT上の根ノードに対応付ける集合を設定する。根ノードには、その下位に全ての葉ノードが連結されているため、全ての端末装置122の一部又は全部が含まれる部分集合を要素に持つ集合が対応付けられる。つまり、根ノードに対応付ける集合として、集合(1→n)と集合(2←n)とが設定される。例えば、図3の根ノードには、集合(1→64)と集合(2←64)とが対応付けられる。

[0084] この対応付けは、以下の理由による。上記の定義により、集合(1→64)は、部分集合[1, 1], ･･･, [1, 64]を要素として含んでいるため、全ての端末装置122(番号1～64)を含む端末装置122のグループを[1, 64]＝{1, ･･･, 64}により表現することができる。同様に、部分集合[1, 15]と部分集合[64, 17]とを用いることによって、番号16の端末装置122を除外した全ての端末装置122を表現することができる。このとき、部分集合[1, 15]は集合(1→64)に含まれており、部分集合[64, 17]は集合(2←64)に含まれている。つまり、根ノードに対応付けられた集合の部分集合を用いることで、根ノードの下位に位置する葉ノード(つまり、端末装置122)の任意の組合せを表現することができるのである。

[0085] （中間ノードに対する集合の対応付け）

次に、BT上の各中間ノードに部分集合を対応付ける。まず、全てのvについて、上記の集合BT_Lに属する中間ノードvに集合$(l_v+1 \leftarrow r_v)$を対応付ける。同様に、全てのvについて、上記の集合BT_Rに属する中間ノードvに集合$(l_v \rightarrow r_v-1)$を対応付ける。図3には、各中間ノードに対応付けられた集合が記載されている。

[0086] 例えば、集合(2←4)が対応付けられた中間ノードを参照すると、この中間ノードの下位に位置する2つの中間ノードには、集合(2←2)と集合(3→3)とが対応付けられている。さらに、2つの中間ノードの下位には、番号1～4の葉ノードが連結されている。そこで、番号3を除外した葉ノードの組合せを表現する場合には、{[1, 1], [2, 2], [4, 4]}又は{[1, 2], [4, 4]}という部分集合の組を対応付ければよい。部分集合

[1, 1]及び[1, 2]は、根ノードに割り当てられた集合(1→64)の要素であり、部分集合[2, 2]及び[4, 4]は、それぞれ、集合(2←2)及び(2←4)の要素である。つまり、各中間ノードに対応付けられた集合の部分集合を用いることで、葉ノード(端末装置122)の所望の組合せを表現することができる。

[0087] 上記の通り、AI05方式では、BTを用いて端末装置122の組合せを表す部分集合の組を定義している。なお、上記の部分集合により形成された全体集合のことをセットシステムSSと呼ぶことにする。また、セットシステムSSは、下式(1)のように数学的に表現される。

[0088] [数1]

$$SS=\left\{\bigcup_{v\in BT_L}(l_v+1\leftarrow r_v)\right\}\cup\left\{\bigcup_{v\in BT_R}(l_v\rightarrow r_v-1)\right\}\cup(1\rightarrow n)\cup(2\leftarrow n)$$

・・・(1)

[0089] 以上、AI05方式における二分木構造の形成方法について説明した。AI05方式の基本コンセプトは、上記の各部分集合に対して、コンテンツ又はコンテンツ鍵を暗号化するための複数のセット鍵を生成し、各セット鍵によりコンテンツ又はコンテンツ鍵を暗号化して所定の端末装置122に対して配信することにある。これまでの記載からはあまり明示的ではないかもしれないが、上記の規則に従って部分集合を定義したことにより、端末装置122の組合せを効率的に分類する手段が提供可能となる。以下では、上記の部分集合を利用してセット鍵を生成するアルゴリズムについて説明する。

[0090] (有向グラフの生成)

ここで、図4を参照しながら、セット鍵を生成するためのアルゴリズムについて説明する。このアルゴリズムは、複数の有向枝により形成される有向グラフによって表現される。そこで、この有向グラフの生成方法について詳細に説明する。まず、コンテンツ鍵を暗号化するセット鍵と、セット鍵を生成するための中間鍵とについて説明する。

[0091] AI05方式では、セット鍵を生成するために擬似乱数生成器PRSGを用いる。このPRSGは、ある部分集合S_0に対応する中間鍵$t(S_0)$が入力されると、部分集合S_0に対応するセット鍵$k(S_0)$と、部分集合S_1, S_2, ・・・, S_kに対応する中間鍵$t(S_1)$, $t(S_2)$,

・・・, t(S_k)とを出力する。ここで、部分集合S_0と、他の部分集合S_1, ・・・, S_kとの関係は、後述する有向グラフにより規定される。

[0092] なお、集合S_0, S_1, ・・・, S_kは、上記のセットシステムSSを構成する部分集合のいずれかであり、上記の通り、端末装置122の組合せを表現するものである。AI05方式の特徴は、PRSGの入力(例えば、t(S_0))と出力(例えば、k(S_0), t(S_1), ・・・, t(S_k))との関係を規定するロジックが表現された有向グラフの形状にある。そこで、AI05方式に係る有向グラフの生成方法について説明する。まず、以下で用いる記号等を定義する。

[0093] (各種定義)

・部分集合S_iに対応する中間鍵 : t(S_i)

・部分集合S_iに対応するセット鍵 : k(S_i)

・コンテンツ鍵 : mek

・擬似乱数生成器 : PRSG

・有向枝 : E

・有向パス(経路) : P

・有向グラフ : H

・部分集合S_iに対応する座標点を始点とする有向枝の数:d

[0094] なお、集合(i→j)、又は集合(i←j)に対応するAI05方式の有向グラフをH(i→j)、又はH(i←j)と表記する。また、有向パスPは、上記の鍵生成経路情報の一例である。さらに、PRSGの入出力を下式(2)のように表記する。これは、PRSGに中間鍵t(S_0)が入力された結果、セット鍵k(S_0)と、複数の中間鍵t(S_1), ・・・, t(S_d)とが出力されたことを示す。

[0095] [数2]

$$t(S_1)\,||\,\cdots\,||\,t(S_d)\,||\,k(S_0) \leftarrow PRSG(t(S_0)) \quad \cdots(2)$$

[0096] (アルゴリズム)

まず、パラメータk(kは自然数)を決定する。但し、簡単のために、k | log(n)(以下、logの底は2)とする。パラメータkは、結果的に端末装置122が保持すべき中間鍵

の個数、及び端末装置122がセット鍵を生成するのに必要な計算量に関係する。従って、パラメータkは、実施の態様に応じて適宜設定されるべきパラメータである。図4の例ではk＝6と設定している。

[0097] ここで、図4を参照しながら、ある中間ノードvに対応する有向グラフH($l_v \rightarrow r_v - 1$)に関し、有向グラフの生成方法について具体的に説明する。

[0098] (ステップ1)

まず、有向グラフH($l_v \rightarrow r_v - 1$)を構成するための水平座標軸を設定する。当該水平座標軸の各座標点には、集合($l_v \rightarrow r_v - 1$)を構成する各部分集合S_iが対応付けられる。但し、各座標点に対応付けられる部分集合S_iは、左から右に向かって包含関係が大きくなるように配置される。例えば、有向グラフH(5→7)＝H({[5, 5], [5, 6], [5, 7]})を例に挙げると、水平座標軸の座標点には、左から順に部分集合[5, 5], [5, 6], [5, 7]が対応付けられる。

[0099] また、図4を参照すると、各有向グラフHが形成される水平座標軸に対して直交する複数の縦線z(z＝1～64)が描かれている。この縦線zと有向グラフHとの交点が上記の座標値を表している。例えば、有向グラフH($l_v + 1 \leftarrow r_v$)と縦線zとの交点は、部分集合[r_v, z]に対応付けられた座標点を表し、有向グラフH($l_v \rightarrow r_v - 1$)と縦線zとの交点は、部分集合[l_v, z]に対応付けられた座標点を表す。以下、部分集合S_iに対応付けられた座標点のことを座標点S_iと表記することがある。

[0100] 上記の規則に則って水平座標軸が設定された後、水平座標軸上の最左に位置する座標点の左側に1つの仮座標点を設定する。さらに、水平座標軸の最右に位置する座標点の右側に1つの仮座標点を設定する。そして、左端の仮座標点を始点とし、右端の仮座標点を終点とする。なお、左端に位置する仮座標点から右端に位置する仮座標点までの長さL_vは$L_v = r_v - l_v + 1$となる。

[0101] (ステップ2)有向グラフH($l_v \rightarrow r_v - 1$)を形成する有向枝を設定する。

(2－1)$n^{(x-1)/k} < L_v \leqq n^{x/k}$を満たす整数xを算出する。但し、整数xは、$1 \leqq x \leqq k$である。

(2－2)カウンタiを0からx－1まで動かしながら、次の操作を繰り返し実行する。水平座標軸上の始点から開始し、有向枝の終端が水平座標軸上の終点に到達する

か、或いは、次に形成される有向枝の終端が水平座標軸上の終点を超えるまで、その座標点から$n^{i/k}$だけ離れた座標点に延びる右向きの有向枝（つまり、その座標点から$n^{i/k}$だけ離れた座標点へのジャンプ）を繰り返し生成する。

[0102] （ステップ3）

仮座標点を始点又は終点とする有向枝を全て削除する。

[0103] （ステップ4）

ある座標点に到達する有向枝が複数ある場合、最長の有向枝のみを残して他の有向枝を全て削除する。

[0104] 上記のアルゴリズム（ステップ1～ステップ4）を実行することで、有向グラフH（$l_v \rightarrow r_v - 1$）を構築することができる。

[0105] ここで、図4の有向グラフH（33→63）を例に挙げて有向グラフの構成について具体的に説明する。有向グラフH（33→63）は、複数のアーチ状の曲線と、各アーチ状の曲線の一端に接続されて水平方向に延伸した直線とにより構成される。このアーチ状の曲線と水平方向に延伸した直線とが有向枝である。そして、各有向枝の端部と縦線との交点が水平座標軸の座標点である。また、連結した複数の有向枝により形成される座標点間の経路のことを有向パスと呼ぶことにする。

[0106] なお、有向グラフH（33→63）の上側に表示された白抜きの矢印は、有向枝の方向を示している。この有向グラフ（33→63）は、$l_v = 33$、$r_v = 64$、$k = 6$、$n = 64$のケースにおいて、上記のアルゴリズムを実行した結果として得られたものである。なお、図4の最下段に描かれた黒丸は、左からそれぞれ、有向グラフH（2←2），・・・，H（63→63）を表している。

[0107] 上記のアルゴリズムは、右向きの有向グラフH（$l_v \rightarrow r_v - 1$）を生成するためのものであったが、左向きの有向グラフH（$l_v + 1 \leftarrow r_v$）についても同様のアルゴリズムを適用して生成することが可能である。但し、有向グラフH（$l_v + 1 \leftarrow r_v$）及びH（2←n）を形成する水平座標軸を設定する場合、水平座標軸上に右から左に向かって包含関係が大きくなるように部分集合S_iを配列する点、及び有向枝の向きを左向きにする点に注意する必要がある。

[0108] 以上、AI05方式に係る有向グラフHの生成方法について説明した。以下では、有

向グラフHを用いてセット鍵を生成するロジックについて説明する。

[0109] （セット鍵の生成）

AI05方式では、セットシステムSSを構成する各部分集合S_iに対応する各セット鍵k(S_i)を用いてコンテンツ鍵mekが暗号化される。また、上記の通り、有向グラフHの各座標点は、端末装置122の組合せを表す部分集合S_iに対応する。そして、セット鍵k(S_i)、及び中間鍵t(S_i)は、上記の各部分集合S_iに対応付けられている。これらの対応関係を踏まえ、有向グラフHに基づいてセット鍵k(S_i)を生成する方法について説明する。

[0110] 以下、座標点S_0を始端とする1本以上の有向枝の終端が示す座標点を当該有向枝の始端S_0に近い順（有向枝が短い順）にS_1, S_2, ・・・, S_kと表現する。但し、座標点S_0を始端とする有向枝の本数がq本（q＜k）である場合、座標点$S_{(q+1)}$, $S_{(q+2)}$, ・・・, S_kはダミーとしてカウントするが実際には使用しない。なお、上記の（ステップ2－2）における繰り返し処理の回数がx回（1≦x≦k）であるため、有向グラフHの各座標点を始端とする有向枝の本数は最大でk本である。

[0111] AI05方式によると、λビットの入力に対して（k＋1）＊λビットを出力するPRSGを利用してセット鍵k(S_i)を生成する。このPRSGは、座標点S_0に対応する中間鍵t(S_0)を入力すると、座標点S_0を始端とする有向枝が到達する各座標点（例えば、座標点S_1, S_2, ・・・, S_k）に対応する中間鍵t(S_1), t(S_2), ・・・, t(S_k)と、入力した中間鍵（S_0）に対応するセット鍵k(S_0)とが出力される。つまり、t(S_1)｜｜・・・｜｜t(S_k)｜｜k(S_0)←PRSG(t(S_0))となる。そこで、PRSGの出力を左からλビット毎に区切ることにより、中間鍵t(S_1), t(S_2), ・・・, t(S_k)と、セット鍵k(S_0)とを生成することができる。

[0112] 例えば、図4を参照し、有向グラフH（1→64）の座標点S_0＝[1, 8]（左端から8番目の座標点）に注目すると、座標点S_0からは4本の有向枝が出ていることが分かる。この有向枝の終点は、それぞれ、座標点S_1＝[1, 9], S_2＝[1, 10], S_3＝[1、12], S_4＝[1、16]である。そこで、中間鍵t(S_0)をPRSGに入力すると、セット鍵k(S_0)と、中間鍵t(S_1), t(S_2), t(S_3), t(S_4)とを生成することができる。さらに、中間鍵t(S_4)をPRSGに入力することにより、セット鍵k(S_4)と、S_{11}＝[1, 17], S_{12}＝[1, 18], S_{13}

$=[1, 20]$, $S_{14}=[1, 24]$, $S_{15}=[1, 32]$に対応する中間鍵$t(S_{11})$, $t(S_{12})$, $t(S_{13})$, $t(S_{14})$, $t(S_{15})$とを生成することができる。このように、PRSGを繰り返し用いることによって複数のセット鍵を算出することができる。

[0113] 上記の通り、所定の中間鍵$t(S_0)$を保持していると、有向グラフHに基づいて中間鍵とセット鍵とを生成することが可能になる。しかし、有向グラフHの情報を参照できない場合には、所定の中間鍵$t(S_0)$をPRSGに入力して生成される中間鍵又はセット鍵が不明であるため、所望のセット鍵を生成することが困難である。この問題に対する解決策を提供するのが本実施形態の目的である。これについては後述する。

[0114] これまで、中間鍵を利用する鍵生成方法について説明したが、既存のAI05方式においても、後述する本実施形態においても中間鍵を利用する構成は必須ではない。そもそも、中間鍵は、安全性を高める目的で使用しているのであって、安全性に格段の注意を払わなくてもよい場面、又はセット鍵生成のための演算量を減らしたい場合等においては、中間鍵を使わずに、セット鍵$k(S_0)$から別のセット鍵$k(S_1)$等を直接的に算出可能な構成にしてもよい。例えば、セット鍵$k(S_0)$がPRSGに入力されると、座標点S_0から伸びる有向枝の到達先に対応するセット鍵$k(S_1)$, $k(S_2)$, $k(S_3)$, $k(S_4)$が出力されるように構成してもよい。

[0115] 以上、セット鍵の生成方法について説明した。上記の例から容易に理解される通り、ある中間鍵を保持していると、その中間鍵を利用し、PRSGを反復して実行することにより、その中間鍵に対応する座標点から伸びた有向枝の鎖によって到達可能な全ての座標点に対応する中間鍵とセット鍵とを導き出すことができるのである。従って、各端末装置122は、自己が要素として含まれる部分集合に対応する中間鍵を全て導出できる最低限の中間鍵を保持していればよいことになる。

[0116] なお、鍵配信サーバ102は、各有向グラフHの先頭座標点(以下、ルートと呼ぶ)に対応する中間鍵を利用し、PRSGによる演算を繰り返し実行することにより、各有向グラフを構成する有向枝が到達可能な全ての座標点に対応するセット鍵を導出することができる。

[0117] 従って、鍵提供システム100の管理者は、鍵提供システム100のセットアップ時に、例えばλビットの乱数を生成し、鍵配信サーバ102において各有向グラフHのルート

の中間鍵として設定すればよい。上記の有向グラフHのルートとは、その座標点から有向枝が出ているが、その座標点に到達することのない座標点のことを言う。例えば、図4の有向グラフH(1→64)のルートは、水平座標軸の左端に位置する座標点[1, 1]である。

[0118] 以上、セット鍵の生成方法について説明した。この方法は、コンテンツ又はコンテンツ鍵の送信者側である鍵配信サーバ102がコンテンツ又はコンテンツ鍵を暗号化するためのセット鍵と、各端末装置122に配信する中間鍵とを生成する際に用いられるだけでなく、受信者側の端末装置122においても、自己が予め保持する中間鍵を利用して所望のセット鍵を生成するために用いられる。

[0119] (中間鍵の配信方法)

次いで、鍵配信サーバ102が各端末装置122に対して所定の中間鍵を配信する方法について説明する。なお、各端末装置122に対しては、その端末装置122が含まれる全ての部分集合に対応するセット鍵を導出可能な複数の中間鍵が予め与えられている。逆に、その端末装置122に対し、当該端末装置122が含まれていない部分集合に対応するセット鍵を導出することが可能な中間鍵を与えてはならないし、当該端末装置122に与える中間鍵の数が最小限になる方が好ましい。

[0120] そこで、鍵配信サーバ102は、契約者uの端末装置122が含まれる部分集合に対応する座標点に到達可能な有向グラフHを全て抽出する。そのうち、有向グラフHのルートに対応する部分集合に契約者uの端末装置122が含まれる場合は、そのルートに対応する中間鍵のみを契約者uの端末装置122に与える。

[0121] また、有向グラフHのルート以外の座標点に対応する部分集合のいずれかに契約者uの端末装置122が含まれる場合は、契約者uの端末装置122が部分集合S_0に含まれ、かつ、部分集合S_0の親である部分集合parent(S_0)に含まれない部分集合S_0を抽出する。そして、その部分集合S_0に対応する中間鍵t(S_0)を契約者uの端末装置122に対して与える。

[0122] つまり、有向グラフHのルート以外の複数の座標点に対応する部分集合に契約者uの端末装置122が含まれる場合は、各座標点に到達する有向枝の始端を参照し、各座標点の始端に対応する部分集合が契約者uに対応する端末装置122を含まな

いような座標点を選択する。この座標点に対応する部分集合をS_0とし、座標点S_0に到達する有向枝の始端(親)に対応する部分集合をparent(S_0)とすると、部分集合parent(S_0)を含まない座標点S_0に対応する中間鍵t(S_0)を契約者uの端末装置122に与えればよいことになる。

[0123] もし、そのような座標点S_0が複数個存在する場合は、それぞれの中間鍵t(S_0)を契約者uの端末装置122に与える。なお、座標点の親子関係は、有向枝により規定される。つまり、有向枝の始端が終端の親となり、有向枝の終端が始端の子となる。また、座標点S_0の親をparent(S_0)と表記する。もちろん、座標点S_0が有効グラフHのルートである場合には座標点S_0の親は存在しない。また、有効グラフHのルートではない場合には座標点S_0の親はただ1つ存在する。

[0124] ここで、図4の例を参照しながら、中間鍵の配信方法について具体的に説明する。

[0125] (例1)

契約者1の端末装置122に対して配信される中間鍵について考える。まず、契約者1の端末装置122が含まれる部分集合に到達可能な有向グラフHを抽出する。図4を参照すると、そのような有向グラフHは、有向グラフH(1→64)のみであることが分かる。そして、契約者1の端末装置122は、有向グラフH(1→64)のルートに対応する部分集合[1, 1]に属している。従って、契約者1の端末装置122には、中間鍵t([1, 1])が配信される。

[0126] (例2)

契約者3の端末装置122に対して配信される中間鍵について考える。まず、契約者3の端末装置122が含まれる部分集合に到達可能な有向グラフHを抽出する。図4を参照すると、そのような有向グラフHは、有向グラフH(1→64), H(2←64), H(2←32), H(2←16), H(2←8), H(2←4), H(3→3)であることが分かる。まず、有向グラフH(1→64)について検討すると、契約者3の端末装置122は、有向グラフH(1→64)のルートに対応する部分集合[1, 1]に含まれていないことが分かる。

[0127] しかし、契約者3の端末装置122は、3番目の座標点以降の部分集合[1, 3], [1, 4], ・・・, [1, 64]に含まれている。そこで、これらの座標点の親の部分集合を参照すると、親の部分集合に契約者3の端末装置122を含まない座標点は、[1, 3]及び

[1, 4]のみであることが分かる。従って、座標点[1, 3], [1, 4]の親parent([1, 3])及びparent([1, 4])に該当する座標点[1, 2]は、契約者3の端末装置122を含んでいないことが分かる。

[0128] その結果、契約者3の端末装置122には、有向グラフH(1→64)に対応する中間鍵t([1, 3])及びt([1, 4])が配信される。同様に、他の有向グラフH(2←64), H(2←32), H(2←16), H(2←8), H(2←4), H(3→3)についても中間鍵が選択されて契約者3の端末装置122に配信される。結局、契約者3の端末装置122には、合計8個の中間鍵が配信される。

[0129] 次に、図5を参照しながら、鍵配信サーバ102が各端末装置122に中間鍵を配信する処理について簡単に説明する。図5は、システムをセットアップする際に鍵配信サーバ102が各端末装置122に中間鍵を配信する処理を表した流れ図である。

[0130] 図5を参照すると、鍵配信サーバ102は、契約者数n、セット鍵及び中間鍵のビット数λ、所定のパラメータk、及びPRSGによる擬似乱数生成アルゴリズム等を決定し、全ての端末装置122に対して公開する(S102)。次いで、鍵配信サーバ102は、端末装置122の集合を所定の部分集合に分けた後、その和集合によって表現されるセットシステムSS(上式(1))を決定して全ての端末装置122に対して公開する(S104)。次いで、鍵配信サーバ102は、複数の有向枝Tにより形成される有向グラフHを決定し、その情報の一部又は全部を全ての端末装置122に対して公開する(S106)。次いで、セットシステムSSを構成する各部分集合に対応する中間鍵を決定する(S108)。そして、各端末装置122に対し、各端末装置122が有向グラフに基づいて所望のセット鍵を導出するために必要な中間鍵を配布する(S110)。

[0131] 以上、中間鍵の配信方法について説明した。この配信方法を用いると、各許諾契約者の端末装置122がセット鍵を生成するために必要な中間鍵を効率的に配信することが可能になり、鍵配信サーバ102と端末装置122と間の通信量、及び各端末装置122が鍵の保持に要するメモリ量を節約することができる。

[0132] (コンテンツ鍵の配信方法)

次に、鍵配信サーバ102により暗号化されたコンテンツ鍵mekの配信方法について説明する。

[0133] まず、鍵配信サーバ102は、許諾契約者の端末装置122のみが生成可能なセット鍵を用いてコンテンツ鍵mekを暗号化する。鍵配信サーバ102は、排除すべき契約者(以下、排除契約者)の端末装置122が含まれる集合Rを決定し、全契約者1～nの端末装置122が含まれる集合Nから集合Rを除外した集合N＼Rを決定する。

[0134] そして、セットシステムSSを構成する部分集合の中から1又は複数の部分集合S_i(i＝1, 2, ･･･, m)を選択し、選択された部分集合を用いて集合N＼R＝S_1∪S_2∪･･･∪S_mを表現する。このとき、部分集合S_iの組合せは多数存在するが、mが最小となるような部分集合S_iを選択する方が望ましい。

[0135] 鍵配信サーバ102は、上記の部分集合S_iを選択した後、各部分集合S_iに対応するセット鍵k(S_i)を用いてコンテンツ鍵mekを暗号化し、セット鍵k(S_1)、k(S_2), ･･･, k(S_m)によって暗号化されたm個のコンテンツ鍵mekを生成する。そして、鍵配信サーバ102は、m個の暗号化されたコンテンツ鍵mekが全契約者1～nの端末装置122に対して配信する。このとき、鍵配信サーバ102は、集合N＼Rの情報、及びm個の部分集合S_iの情報の一方又は両方も同時に各端末装置122に対して配信する。

[0136] 次に、図6を参照しながら、鍵配信サーバ102により暗号化されたコンテンツ鍵mekの配信処理について簡単に説明する。図6は、コンテンツ鍵の配信処理の流れを示す説明図である。

[0137] 図6を参照すると、鍵配信サーバ102は、排除契約者の集合Rを決定し、許諾契約者の集合N＼Rを決定する(S112)。次いで、鍵配信サーバ102は、セットシステムSSを構成する部分集合から、和集合がN＼Rとなるm個の部分集合S_i(i＝1, 2, ･･･, m)を選択する(S114)。次いで、鍵配信サーバ102は、選択された各部分集合S_iに対応するセット鍵k(S_i)を用いてコンテンツ鍵mekをそれぞれ暗号化する(S116)。次いで、鍵配信サーバ102は、集合N＼R又は各部分集合S_iを表す情報と、m個の暗号化されたコンテンツ鍵mekとを全ての端末装置122に対して配信する(S118)。

[0138] 以上、鍵配信サーバ102によるコンテンツ鍵mekの暗号化方法、及び配信方法について説明した。上記の暗号化方法を用いると、暗号化に要するセット鍵数が最小限となるように部分集合S_iを選択することができる。そのため、コンテンツ鍵mekを暗号化する際に、暗号化に要する計算量を低減できると共に、配信すべき暗号化され

たコンテンツ鍵mekの数を低減させることが可能になり、通信量の低減化も実現されうる。

[0139] （コンテンツ鍵の復号方法）

次に、各端末装置122におけるコンテンツ又はコンテンツ鍵の復号処理について説明する。端末装置122は、上記鍵配信サーバから受信した集合N＼R又はm個の部分集合S_iの情報と、m個の暗号化されたコンテンツ鍵とに基づいてコンテンツ鍵mekを復号する。

[0140] 端末装置122は、鍵配信サーバ102から暗号化されたコンテンツ鍵mekと、集合N＼Rを表す情報又はm個の部分集合S_iを表す情報とを受信する。次いで、端末装置122は、これらの情報を解析して、自身がm個の部分集合S_iのいずれかに含まれるか否かを判断する。次いで、端末装置122は、自身がいずれの部分集合にも含まれないと判断した場合、自身が排除契約者の端末装置122であると判断して復号処理を終了する。逆に、自身が含まれる部分集合S_iが発見された場合、端末装置122は、上記のPRSGを利用して当該部分集合S_iに対応するセット鍵$k(S_i)$を導出する。但し、端末装置122が利用するPRSGの構成は、上記の鍵配信サーバ102が暗号化に利用したPRSGの構成と同様である。

[0141] なお、端末装置122は、システムのセットアップに際し、鍵配信サーバ102から上記の部分集合S_iに対応する中間鍵$t(S_i)$又は当該中間鍵$t(S_i)$を導出可能な中間鍵$t(S_j)$が予め配信されているものとする。従って、端末装置122は、保持している中間鍵$t(S_i)$又は$t(S_j)$をPRSGに入力し、上記部分集合S_iに対応するセット鍵$k(S_i)$を導出することが可能である。このとき、端末装置122は、有向グラフの情報を参照してPRSGの処理を繰り返し実行し、上記のセット鍵$k(S_i)$を算出する必要があるかもしれない。次いで、端末装置122は、導出したセット鍵$k(S_i)$を用いて暗号化されたコンテンツ鍵mekを復号する。

[0142] ここで、再び図4を参照する。図4を参照しながら、端末装置122における上記セット鍵$k(S_i)$の導出方法について具体例を挙げて説明する。

[0143] （例1）

図4に示した有向グラフHに基づいて、契約者3の端末装置122が部分集合[1，8

]に対応するセット鍵を導出する過程について考える。なお、鍵配信サーバ102は、システムセットアップの際、契約者3の端末装置122に対して予め部分集合[1, 4]の中間鍵を配信している。

[0144] まず、有向グラフH(1→64)を参照すると、座標点[1, 4]から座標点[1, 8]に延びる有向枝が存在する。この有向枝は、座標点[1, 4]を始端とする有向枝のうち3番目に距離が短いものである。そこで、契約者3の端末装置122は、座標点[1, 4]に対応する中間鍵t([1, 4])をPRSGに入力して得られる出力のうち、先頭から第3番目のλビットの部分を抽出する。出力の第3番目のλビット部分が部分集合[1, 8]に対応する中間鍵t([1, 8])なのである。そこで、契約者3の端末装置122は、PRSGの出力から中間鍵t([1, 8])を抽出した後、中間鍵t(S[1, 8])を再度PRSGに入力して得られた出力の最終λビットを抽出する。出力の最終λビットが所望のセット鍵k([1, 8])なのである。以上の処理により、契約者3の端末装置122は、所望のセット鍵k([1, 8])を生成することができる。

[0145] (例2)

同様に、図4の有向グラフHに基づいて、契約者1の端末装置122がセット鍵k([1, 8])を生成する場合について考える。契約者1の端末装置122は、部分集合[1, 1]に対応する中間鍵t([1, 1])を予め保持している。そこで、契約者1の端末装置122は、中間鍵t([1, 1])をPRSGに入力して得られた出力の先頭から第1番目のλビットの部分(中間鍵t([1, 2]))を抽出する。次いで、契約者1の端末装置122は、中間鍵t([1, 2])を再度PRSGに入力して得られた出力の先頭から第2番目のλビットの部分(中間鍵t([1, 4]))を抽出する。さらに、契約者1の端末装置122は、中間鍵t([1, 4])を再度PRSGに入力して得られた出力の先頭から第3番目のλビットの部分(中間鍵t([1, 8]))を抽出する。最後に、契約者1の端末装置122は、中間鍵t([1, 8])をPRSGに入力して得られた出力の最終λビット(セット鍵k([1, 8]))を抽出して、所望のセット鍵k([1, 8])を取得することができる。

[0146] 次に、図7を参照しながら、各端末装置122における暗号化されたコンテンツ鍵mekの復号処理について説明する。図7は、各端末装置122におけるコンテンツ鍵の復号処理の流れを示す説明図である。

[0147] 図7を参照すると、端末装置122は、鍵配信サーバ102からm個の暗号化されたコンテンツ鍵mekと、集合N＼Rを表す情報又はm個の部分集合S_i（i＝1，2，・・・，m）を表す情報とを受信する（S120）。次いで、端末装置122は、自身が含まれる部分集合S_iを検索し（S122）、自身がm個の部分集合S_iのいずれかに含まれているか否かを判断する（S124）。

[0148] 自身が含まれる部分集合S_iが存在する場合、端末装置122は、上記のPRSGを利用して、その部分集合S_iに対応するセット鍵k（S_i）を導出する（S126）。次いで、端末装置122は、導出したセット鍵k（S_i）を用いて暗号化されたコンテンツ鍵mekを復号する（S128）。

[0149] 一方、自身がいずれの部分集合S_iにも含まれないと判断した場合、端末装置122は、自身が許諾契約者の端末装置122ではない旨（排除契約者である旨）を表示出力し（S130）、コンテンツ鍵の復号処理を終了する。

[0150] 以上、端末装置122におけるコンテンツ鍵の復号方法について説明した。上記の復号方法には、端末装置122側にも有向グラフの情報とPRSGとが必要とされる。しかし、有向グラフの情報を全て端末装置122が保持しておくことは端末装置122のメモリ量を大きく圧迫するという点で困難であり、また、端末装置122が全ての有向グラフを生成することも端末装置122の演算負荷を増大させるという点で困難である。もちろん、有向グラフの情報を全て配信することも通信量の著しい増大又は配信媒体の記憶容量の圧迫という点から困難である。本実施形態に係る鍵提供システム100は、こうした問題点を解決する手段を提供するものであり、その特徴については後述する。

[0151] （AI05方式のまとめ）

以上、本実施形態を適用可能なAI05方式について説明してきた。このAI05方式を用いると、各端末装置122が保持すべき中間鍵の個数をO（k＊log（n））に抑えることができる。また、セット鍵の生成に要する計算量（PRSGの動作回数）を（2k－1）＊（$n^{1/k}$－1）程度又はそれ以下に抑えることができる。しかし、本件出願人が既に指摘している通り、AI05方式には効率化の観点からいくつかの改善の余地が残されている。例えば、A06（A）方式では端末装置122が保持すべき鍵数を削減することに

成功しており、A06(B)方式では端末装置122が鍵生成に要する演算量を低減させることに成功している。そして、A06(A+B)方式において端末装置122の保持すべき鍵数と鍵生成に要する演算量とをバランス良く低減させることに成功している。本実施形態の特徴は、端末装置122が鍵生成する際に必要な有向グラフの情報を如何にして提供するかという点にあるため、少なくとも上記の各方式の全てに適用が可能である。

[0152] (A06(A+B)方式)

次に、本実施形態を適用可能なA06(A+B)方式について説明する。上記の通り、A06(A+B)方式は、AI05方式に比べて効率的な鍵配信を実現可能な方式である。従って、本実施形態を適用するに当り、A06(A+B)方式を適用する方がより効率的である。

[0153] A06(A+B)方式について説明するに先立ち、鍵配信の効率について簡単に説明する。まず、端末装置122が所望の鍵生成に要する計算量は、所望の中間鍵を導出するためにPRSGを実行する回数に依存している。この最悪値は、有向グラフHを辿りながら、ルートから最も遠い末尾の座標点(有向枝が出ていないリーフ)に到達するまでに存在する有向枝の本数に対応する。図4の有向グラフH(1→64)を参照すると、ルート[1, 1]から末尾の座標点[1, 64]に到達するまでに11本の有向枝を経由しており、中間鍵t([1, 1])を保持する端末装置122が中間鍵t([1, 64])を導出するためにPRSGを11回も実行しなければならないことを意味している。従って、水平座標軸上の全ての座標点に到達可能な経路を確保しつつ、有向グラフの最長パスを構成する有向枝数を低減させることができれば、端末装置122の演算量を低減させることができるのである。この課題に対する一つのアプローチがA06(B)方式であり、これを更に改良したものがA06(A+B)方式である。そこで、本実施形態をA06(A+B)方式に適用する場合を例に挙げて詳細に説明する。

[0154] [鍵配信サーバ102の構成]

まず、図8を参照しながら、本実施形態に係る鍵配信サーバ102の構成について説明する。図8は、本実施形態に係る鍵配信サーバ102及び端末装置122の構成を示す説明図である。

[0155] 図8を参照すると、鍵配信サーバ102は、主に、木構造設定部104と、座標軸設定部106と、仮有向グラフ生成部108と、有向グラフ生成部110と、初期中間鍵設定部112と、鍵生成部114と、暗号化部116と、通信部118と、部分集合決定部120とにより構成される。また、木構造設定部104と、座標軸設定部106と、仮有向グラフ生成部108と、有向グラフ生成部110とを纏めて、鍵生成ロジック構築ブロックと呼ぶことにする。同様に、初期中間鍵設定部112と、鍵生成部114とを纏めて、鍵生成ブロックと呼ぶことにする。なお、座標軸設定部106、仮有向グラフ生成部108、有向グラフ生成部110は、上記の集合関係情報生成部又は集合関係情報取得部の一例である。また、通信部118は、上記の鍵生成経路情報提供部又は暗号情報提供部の一例である。

[0156] [鍵生成ロジック構築ブロック]

まず、鍵生成ロジック構築ブロックについて詳細に説明する。

[0157] (木構造設定部104)

まず、木構造設定部104について説明する。木構造設定部104は、上記AI05方式と同様の二分木構造(図3を参照)を生成することができる。まず、木構造設定部104は、番号1～n(nは自然数)のn個の葉ノードと、根ノードと、根ノード及び葉ノード以外の複数の中間ノードとにより形成される二分木構造を設定する。次いで、木構造設定部104は、ある中間ノードv又は根ノードvの下位に配置された複数の葉ノードのうち、左端に位置する前記葉ノードの番号をl_vとし、右端に位置する前記葉ノードの番号をr_vと設定する。次いで、木構造設定部104は、根ノードに対して集合(1→n)と集合(2←n)とを割り当てる。次いで、木構造設定部104は、上記の二分木を形成する任意の中間ノードvの対し、中間ノードvが親ノードの左側に位置する場合には集合(l_v +1←r_v)を対応付け、逆に、中間ノードvが親ノードの右側に位置する場合には集合(l_v →r_v −1)を対応付ける。

[0158] (座標軸設定部106)

次に、座標軸設定部106について説明する。座標軸設定部106は、上記AI05方式と類似した規則に基づいて水平座標軸を設定する。まず、座標軸設定部106は、複数の水平座標軸を設定する。次いで、座標軸設定部106は、集合(1→n−1)に

含まれる複数の部分集合を左側から順に右方向に向かって包含関係が大きくなるように、一つの水平座標軸上の各座標点に対応付ける。同様に、座標軸設定部106は、集合($l_v \rightarrow r_v - 1$)に含まれる複数の部分集合を左側から順に右方向に向かって包含関係が大きくなるように、他の一つの水平座標軸上の各座標点に対応付ける。もちろん、座標軸設定部106は、上記の二分木を形成する中間ノードに対応付けられた全ての集合($l_v \rightarrow r_v - 1$)について同様の処理を繰り返す。

[0159] 次いで、座標軸設定部106は、集合(2←n)に含まれる複数の部分集合を右側から順に左方向に向かって包含関係が大きくなるように、さらに別の一つの水平座標軸上の各座標点に対応付ける。同様に、座標軸設定部106は、集合($l_v + 1 \leftarrow r_v$)に含まれる複数の部分集合を右側から順に左方向に向かって包含関係が大きくなるように、さらに別の一つの水平座標軸上の各座標点に対応付ける。もちろん、座標軸設定部106は、上記の二分木を形成する中間ノードに対応付けられた全ての集合($l_v + 1 \leftarrow r_v$)について同様の処理を繰り返す。

[0160] 次いで、座標軸設定部106は、集合(1→n－1)に対応する水平座標軸の右端に位置する座標点の右側に2つの仮座標点を生成する。次いで、座標軸設定部106は、集合($l_v \rightarrow r_v - 1$)に対応する水平座標軸の右端に位置する座標点の右側に2つの仮座標点を生成する。次いで、座標軸設定部106は、集合(2←n)に対応する水平座標軸と、集合($l_v + 1 \leftarrow r_v$)に対応する水平座標軸の左端に位置する座標点の左側に2つの仮座標点を生成する。

[0161] 以上の処理により、座標軸設定部106は、二分木を形成する全てのノードに対応付けられた集合に対して有向グラフを形成するための水平座標軸を設定することができる。以下、座標軸設定部106により生成された各水平座標軸上に有向グラフを形成する手段について説明する。

[0162] (仮有向グラフ生成部108)

次に、仮有向グラフ生成部108について説明する。仮有向グラフ生成部108は、上記のAI05方式で有向グラフHを生成したのと類似した方法により、仮有向グラフI'を生成する。まず、仮有向グラフ生成部108は、所定の整数kをパラメータとして設定する。次いで、仮有向グラフ生成部108は、$n^{(x-1)/k} < r_v - l_v + 1 \leq n^{x/k}$を満たす整数x

を決定する。次いで、仮有向グラフ生成部108は、集合(1→n－1)及び集合(l_v→r_v－1)に対応する水平座標軸上に、$n^{i/k}$(i＝0～x－1)の長さを有する右方向を向いた有向枝を形成する。次いで、仮有向グラフ生成部108は、集合(2←n)及び集合(l_v＋1←r_v)に対応する水平座標軸上に、$n^{i/k}$(i＝0～x－1)の長さを有する左方向を向いた有向枝を形成する。

[0163] 上記の通り、AI05方式において、部分集合のうちで最も要素数の少ない部分集合(即ち、一人のユーザからなる部分集合)に対応する座標点の隣に配置された仮座標点から有向枝の生成が開始される。これに対し、A06(A＋B)方式では、部分集合のうちで最も要素数の少ない部分集合(即ち、一人のユーザからなる部分集合)に対応する座標点から有向枝の生成が開始される点に注意が必要である。

[0164] 次いで、仮有向グラフ生成部108は、上記の全ての水平座標軸上の有向枝について、水平座標軸上の仮座標点を始端又は終端とする全ての有向枝を消去する。次いで、仮有向グラフ生成部108は、上記の全ての水平座標軸上の全ての座標点について、一つの座標点に到達する有向枝が複数存在する場合、その座標点に到達する複数の有向枝の中から最長の有向枝以外の全ての有向枝を消去する。次いで、仮有向グラフ生成部108は、集合(1→n－1)に対応する水平座標軸上に生成された仮座標点のうち、左側に位置する仮座標点を終端とする長さ1の右向き有向枝を追加する。つまり、仮有向グラフ生成部108は、下式(3)の処理を実行することにより、根ノードに対応付けられた集合(1→n)に対応する仮有向グラフI'(1→n)を生成することができる。

[0165] [数3]

$$E(I'(1\rightarrow n-1))\cup\{([1,\ n-1],[1,\ n])\}$$
・・・(3)

[0166] 以上の処理により、仮有向グラフ生成部108は、AI05方式に比べて長い有向枝により構成される仮有向グラフI'を形成することができる。このアルゴリズムは、A06(B)方式の基本コンセプトに基づくものである。このアルゴリズムを適用することにより、端末装置122が鍵生成に要する演算量を低減させる効果が得られる。

[0167] (アルゴリズム)

ここで、図9を参照しながら、座標軸設定部106及び仮有向グラフ生成部108により実行される処理の流れについて簡単に整理する。なお、図9に示す流れ図は、一例として、集合($l_v \rightarrow r_v - 1$)に対応する仮有向グラフI'($l_v \rightarrow r_v - 1$)の生成方法を示したものである。

[0168] (S140)まず、集合($l_v \rightarrow r_v - 1$)の要素を水平直線上に左から右に包含関係が大きくなるように並べる。そして、最左の座標点を始点とする。さらに、最右の座標点の右に2つの仮座標点を配置する。すると、始点から最右の仮座標点までの長さは、$L_v = r_v - l_v + 1$となる。さらに、$n^{(x-1)/k} < L_v \leqq n^{x/k}$を満たす整数x($1 \leqq x \leqq k$)を算定する。

[0169] (S142)次いで、カウンタiを0～x－1まで動かしながら下記の操作を行う。始点から開始し、その座標点から$n^{i/k}$だけ離れた座標点へのジャンプを続け、仮座標点に到達するか、次のジャンプが仮座標点を超えたところで終了する。その後、各ジャンプに対応する有向枝を生成する。

[0170] (S144)次いで、仮座標点に到達する有向枝を全て消去する。

[0171] (S146)ある座標点Tに到達する有向枝が複数ある場合には、ジャンプの距離が一番長いもののみを残し、それ以外の有向枝は消去する。

[0172] 上記のアルゴリズムを適用することにより、図10に示した仮有向グラフI'を生成することができる。但し、図10の仮有向グラフI'は、葉ノード数n＝64、パラメータk＝6と設定したケースである。以下、この仮有向グラフI'を形成する複数の有向枝の一部を所定の規則に基づいて置換し、有向グラフIを生成するアルゴリズムについて説明する。なお、有向枝の置換処理は、主に、有向グラフ生成部110により実行される。

[0173] (有向グラフ生成部110)

まず、有向グラフ生成部110について説明する。有向グラフ生成部110は、仮有向グラフI'を構成する複数の有向枝の一部を置換して有向グラフIを生成する。まず、有向グラフ生成部110は、仮有向グラフI'に含まれる有向パスのうち、それを構成する有向枝数が最大の有向パスを選択する。その有向パスを最長有向パスLP(Longest Path)と呼ぶことにする。そして、有向グラフ生成部110は、全ての有向パスの有向枝数が最長有向パスLPの有向枝数を超えないという条件の下で、仮有向グラフI'に含まれる有向パスを、より短い有向枝の組で構成される有向パスに置換する。

[0174] （アルゴリズム）

ここで、図11～図14を参照しながら、有向グラフIを生成するアルゴリズムについて詳細に説明する。図11は、有向グラフIを生成する処理の全体的な流れを示した説明図である。図12は、最長有向パスLPを抽出する処理の流れを示した説明図である。図13は、最長有向パスLP以外の有向パスの中から最長の有向パスPLP（Partially Longest Path）を抽出する処理の流れを示した説明図である。図14は、仮有向グラフI'の有向パスをより短い有向枝の組で構成される有向パスに置換する処理を示した説明図である。

[0175] 図11に示すように、まず、有向グラフI'を形成する有向パスの中から最長有向パスLPが抽出される（S150）。次いで、仮有向グラフI'の最長有向パスLP以外の有向パスの中から最長の有向パスPLPが抽出される（S152）。なお、各部分集合に対応する仮有向グラフI'について最長の有向パスPLPが抽出されてもよい。次いで、仮有向グラフI'の有向パスを構成する所定の有向枝が、より短い有向枝に置換される（S154）。このとき、全ての有向パスの有向枝数が最長有向パスLPの有向枝数を超えないように有向枝が置換される。つまり、この置換処理を実行したとしても、AI05方式又はA06（B）方式よりも鍵生成に要する計算量の最悪値が増加しないようにする。

[0176] 以下、図11に示した各ステップについて、より詳細に説明する。

[0177] （S150の詳細）

まず、図12を参照しながら、最長有向パスLPが抽出されるステップ（S160）について詳細に説明する。ここで、以下に示す2つの表記を導入する。

[0178] ・DD_T ： 最長有向パスLPの有向枝数を示す。

・J（a, b）： 長さbの有向枝がa本連続して存在することを示す。

[0179] まず、$t=n^{1/k}-1$とおく。次いで、仮有向グラフI'（1→n）の座標点[1, 1]から座標点[1, n]までの有向パスP（[1, 1], [1, n]）を考える。有向パスP（[1, 1], [1, n]）は、$J(t, n^{(k-1)/k})$, $J(t, n^{(k-2)/k})$, ・・・, $J(t, n^{1/k})$, $J(t, n^{0/k})$と表現される。この有向パスを最長有向パスLPと呼ぶ。このとき、最長有向パスLPの有向枝数DD_Tは、$D_T=k*(n^{1/k}-1)$となる。次いで、最長有向パスLPを構成する全ての有向枝に対

してactiveマークを設定する。

[0180] (S152の詳細)

次に、図13を参照しながら、最長有向パスLPを含む仮有向グラフI'以外の全ての部分集合に対応する仮有向グラフI'について、最長の有向パスPLPを抽出する処理(S162～S176)について説明する。ここで、以下に示す2つの表記を導入する。

[0181] ・CP(Current Path) : 参照中の有向パス(現在パス)

・#JP(CP) : 現在パスの有向枝数

[0182] まず、有向グラフI'の始点から終点への現在パスCPを決定する。このとき、現在パスが有向グラフI'(a→b)に含まれる場合は、有向パスP([a, a], [a, b])を現在パスCPとし、有向グラフI'(a←b)に含まれる場合は、有向パスP([b, b], [b, a])を現在パスCPとする(S162)。次いで、現在パスCPを構成する有向枝のうち、最長の有向枝を選択して、その長さをJとする(S164)。次いで、J≦1か否かを判断する(S166)。

[0183] J≦1である場合、現在パスCPを最長の有向パスPLPと決定して、現在パスCPに含まれる全ての有向枝にactiveマークを設定する(S176)。J＞1である場合、#JP(CP)＋t≦DD_Tか否かを判断する(S168)。#JP(CP)＋t≦DD_Tでない場合、現在パスCPを有向パスPLPと決定して、現在パスに含まれる全ての有向枝にactiveマークを設定する(S176)。#JP(CP)＋t≦DD_Tである場合、J＝$n^{j/k}$となる自然数jを算出する(S170)。

[0184] 次いで、現在パスCPに含まれる長さJの有向枝の中で現在パスCPの始点から最も遠い有向枝を抽出する(S172)。ステップS172で抽出された有向枝の始点から伸びたt個の長さ$n^{(j-1)/k}$の有向枝の直後に$n^{(j-1)/k}$の長さを有する1つの有向枝を追加し、ステップS172で抽出された有向枝を除去し(S174)、ステップS162に戻って上記の処理を繰り返す。

[0185] なお、ステップS162～ステップS174の間に生じるループ処理は、有向グラフI'の始点から終点への有向パスが全て長さ1の有向枝で構成されるか、又は、それ以上の有向枝の置換を実行することで、その有向パスを構成する有向枝数がDD_Tを超えてしまう場合にループ処理を終了する。

[0186] （S154の詳細）

次に、図14を参照しながら、仮有向グラフI'に含まれる有向枝を短い有向枝に置換する処理（S180～S202）について詳細に説明する。

[0187] まず、グラフ中のactiveかつ、未実施（doneマークが付いていない）有向枝のうち、最長の長さJ'を持つ有向枝を抽出する。もし、最大の有向枝が複数存在する場合は、仮有向グラフI'の始点から最も遠い有向枝を選択する（S180）。ここで選択された有向枝をWJ（Working Jump）と呼ぶことにする。また、有向枝WJの始点をWJ_S、終点をWJ_Eと呼ぶことにする。さらに、仮有向グラフI'の始点からWJ_Eまでの有向パスに含まれる有向枝数をDと表記する。

[0188] 次いで、有向枝の長さJ'がJ'≦1であるか否かを判断する（S182）。J'≦1である場合、activeマークの付いていない有向枝を全て消去し、activeマークが付いている有向枝を全て集めたものをE（I（a→b））又はE（I（a←b））と設定する（S202）。逆に、J'≦1でない場合、WJ_SからWJ_E－1までの有向パスを現在パスCPと設定する（S184）。但し、WJ_E－1は、WJ_Eの1つ手前の要素を表す。

[0189] 次いで、現在パスCPに含まれる有向枝の中から最長の有向枝を抽出し、その長さをJとする（S186）。次いで、有向枝の長さJがJ≦1か否かを判断する（S188）。J≦1である場合、現在パスCPに含まれる全ての有向枝にactiveマークを付ける（S198）。そして、WJにdoneマークを付け（S200）、ステップS180の処理に戻る。逆に、J≦1でない場合、#JP（CP）＋t≦DD_T－Dであるか否かを判断する（S190）。#JP（CP）＋t≦DD_T－Dでない場合、ステップS198及びS200の処理を経てステップS180の処理に戻る。#JP（CP）＋t≦DD_T－Dである場合、$J=n^{j/k}$を満たすjを算出する（S192）。

[0190] 次いで、現在パスCPに含まれる長さJの有向枝が複数存在する場合、現在パスCPの始点から最も遠い位置にある有向枝を抽出する（S194）。次いで、ステップS194で抽出された有向枝の始点から伸びた$n^{1/k}-1$個の長さ$n^{(j-1)/k}$の有向枝の直後に$n^{(j-1)/k}$の長さを有する1つの有向枝を追加し、ステップS194で抽出された有向枝を消去する（S196）。そして、ステップS184の処理に戻る。

[0191] 但し、ステップS184～S196の間に生じるループ処理は、WJ_SからWJ_E－1への有

向パスが全て長さ1の有向枝で構成されるか、又は、それ以上の有向枝を置換することによってWJ_SからWJ_E-1への有向パスに含まれる有向枝数がDD_Tを超えてしまう場合に終了する。また、上記のステップS180～S200の間に生じるループ処理は、仮有向グラフI'に含まれる有向枝の中から、doneが設定されておらず、かつ、長さが2以上の有向枝が全てなくなった時点で終了する。

[0192] 以上説明したアルゴリズムを仮有向グラフI'に適用することにより、図15に示す有向グラフIが生成される。この有向グラフIは、契約者数n＝64、パラメータk＝6の場合について生成されたものである。この有向グラフIを用いると、AI05方式に比べ、各端末装置122が鍵生成に要する計算量と、各端末装置122が保持すべき鍵数を低減させることが可能になる。

[0193] ［鍵生成ブロック］

次に、再び図8を参照しながら、鍵生成ブロックの詳細について説明する。鍵生成ブロックは、主に、初期中間鍵設定部112と、鍵生成部114と、暗号化部116とにより構成される。

[0194] （初期中間鍵設定部112）

初期中間鍵設定部112は、論理二分木に含まれる全ての中間ノード及び根ノードの有向グラフIのルートに対応する中間鍵を生成する。例えば、初期中間鍵設定部112は、PRSGにより擬似乱数を発生させて各ルートに対応する中間鍵を設定してもよいし、又は所定の数値により各ルートの中間鍵を設定してもよい。

[0195] （鍵生成部114）

鍵生成部114は、PRSGを利用して中間鍵又はセット鍵を生成する。このとき、鍵生成部114は、AI05方式の有向グラフH、A06（A＋B）方式の有向グラフI、A06（A）方式の有向グラフ、A06（B）方式の有向グラフ、又はその他の方式の有向グラフに基づいて擬似乱数生成演算を実行することにより、所望の中間鍵又はセット鍵を生成することができる。上記の通り、PRSGは、有向グラフを構成する有向枝の始端に対応する中間鍵を入力すると、その中間鍵に対応するセット鍵と、その有向枝の終端に対応する中間鍵とを出力する。有向グラフの水平座標軸上にある一つの座標点から複数の有向枝が伸びている場合には、その座標点に対応する中間鍵を入力す

ると、複数の中間鍵を導出することができる。

[0196] なお、AI05方式では、上式(2)でPRSGの入出力が定義されていたが、本実施形態においては、$t(S_1)||\cdots||t(S_k)||k(S_0)\leftarrow PRSG(t(S_0))$によりPRSGの入出力が定義される。即ち、AI05方式によるPRSGの出力は、入力された中間鍵に対応する座標点を始点とする有向枝の数をdとしたとき、λビットの入力に対して(d+1)λビットの出力を出すように構成されていた。これに対し、本実施形態に係るPRSGは、dの値に関わらず(k+1)λビットの出力を出すように構成される。但し、kはシステムパラメータである。

[0197] 本実施形態において、部分集合S_0に対応する中間鍵$t(S_0)$がそのPRSGに入力された場合、その出力を$t(S_1)||\cdots||t(S_k)||k(S_0)$としている。その出力に含まれる$t(S_1)||\cdots||t(S_k)$の部分は、部分集合$S_0$に対応する座標点を始点とする有向枝の終点である座標点のそれぞれについて、対応する部分集合$S_1, \cdots, S_k$の中間鍵である。また、部分集合S_0に対応する座標点と部分集合S_iに対応する座標点とを結ぶ有向枝の長さが$n^{(i-1)/k}$となる。例えば、部分集合S_0に対応する座標点と部分集合S_iに対応する座標点とを結ぶ有向枝の長さが$n^{2/k}$であれば、$PRSG(t(S_0))$の出力の最初から3番目のλビットの部分が$t(S_i)$になる。もし、部分集合S_0に対応する座標点から長さ$n^{(i-1)/k}$の有向枝が出ていない場合、$t(S_i)$の部分がPRSGから出力されるけれども使用されない。

[0198] 例えば、鍵生成部114は、PRSGに対し、有向グラフI上の座標点S_0に対応する中間鍵$t(S_0)$を入力すると、座標点S_0を始端とする複数の有向枝について、その終端の座標点$S_1, S_2, \cdots, S_m$に対応する中間鍵$t(S_1), t(S_2), \cdots, t(S_m)$と、セット鍵$k(S_0)$とを導出することができる。なお、mは座標点$S_0$から伸びる有向枝の本数を表している。なお、中間鍵を利用しない場合は、例えば、セット鍵$k(S_0)$をPRSGに入力して、複数のセット鍵$k(S_1), k(S_2), \cdots, k(S_m)$を導出するように構成することも可能である。

[0199] (暗号化部116)

暗号化部116は、セット鍵を用いてコンテンツ又はコンテンツ鍵を暗号化して暗号文を生成する。暗号化部116は、セットシステムSSを構成する全ての部分集合のうち

、所定の部分集合に対応する1つ以上のセット鍵を用いてコンテンツ又はコンテンツ鍵を暗号化する。従って、一つのコンテンツ又はコンテンツ鍵に対して複数の暗号文が生成される場合もある。

[0200] [情報生成ブロック]

次に、再び図8を参照しながら、情報生成ブロックの詳細について説明する。情報生成ブロックは、主に、部分集合決定部120と、経路情報生成部121とにより構成される。なお、通信部118についても併せて説明する。

[0201] (部分集合決定部120)

部分集合決定部120は、コンテンツ又はコンテンツ鍵を暗号化するセット鍵を決定する。つまり、部分集合決定部120は、所定の許諾契約者の端末装置122が含まれる少なくとも1つの部分集合を抽出し、各端末装置122に配布されるセット鍵の種類を決定する。例えば、部分集合決定部120は、コンテンツ又はコンテンツ鍵の再生を許諾しない排除契約者の集合(R)、及び全契約者の集合(N)から排除ユーザの集合(R)を除外した許諾契約者の集合(N＼R)を決定する。つまり、セットシステムSSに含まれる部分集合により、許諾契約者の集合($N \setminus R = S_1 \cup S_2 \cup \cdots \cup S_m$)を構成する部分集合の組($S_1, S_2, \cdots, S_m$)を決定する。

[0202] (経路情報生成部121)

経路情報生成部121は、有向グラフに含まれる有向枝の情報を参照し、当該有向グラフの始点から所定の座標点に到達する有向パスの情報を抽出する。所定の座標点とは、部分集合決定部120により選択された各部分集合に対応する座標点である。なお、経路情報生成部121は、上記の鍵生成経路情報抽出部の一例である。

[0203] 既に説明した通り、上記のAI05方式等の鍵配信方式は、全ての端末装置122が有向グラフの情報を保持しているか、又は各端末装置122が各鍵配信方式のアルゴリズムに基づいて有向グラフを算出することを前提としている。しかし、この前提は、端末装置122のメモリ量を圧迫し、演算負荷を著しく増大させるため、現実的ではないという問題がある。

[0204] 例えば、AI05方式の有向グラフH(図16を参照)の場合、契約者3の端末装置122は、部分集合$S_0 = [1, 4]$に対応する中間鍵$t(S_0)$を予め保持している。仮に、部分

集合決定部120が部分集合S＝[1, 8]を選択し、これに対応するセット鍵k(S)を用いてコンテンツ鍵を暗号化した場合を考えると、契約者3の端末装置122は、まず、中間鍵t(S_0)とPRSGとを利用して中間鍵t(S)を導出する必要がある。しかし、これを導出するために、契約者3の端末装置122は、有向グラフH(1→64)上に座標点S_0＝[1, 4]から座標点S_1＝[1, 8]に有向枝が存在するという情報(図16の太線の一部)を保持している必要がある。

[0205] しかし、下式(4)に示す通り、有向グラフH(1→n)上には(n－1)本の有向枝が存在するため、nが大きくなると全ての有向枝の情報を保持するのが困難になる。例えば、1本の有向枝の情報が8Byte程度の情報量で表現できると仮定すると、現実的な契約者数nがn＝2^{32}＝4, 294, 967, 296であるから、有向グラフH(1→n)の情報だけで約32GByteもの記憶容量を必要とする。

[0206] [数4]

$$t\cdot n^{0/k}+t\cdot n^{1/k}+\cdots+t\cdot n^{k-1/k}$$
$$=t\sum_{i=0}^{k-1}t\cdot n^{i/k}$$
$$=n-1$$
・・・(4)

[0207] そこで、本件出願人は、選択した部分集合(上記の例では[1, 8])の情報に加え、その有向グラフの始点から、その部分集合に対応する座標点に到達する有向パスの情報も端末装置122に配信する方式を考案したのである。例えば、上記の例と同様に、部分集合[1, 8]が選択されると、有向グラフH(1→64)の始点[1, 1]から座標点[1, 8]に到達する有向パス(図16の太線)の情報が端末装置122に配信される。この特徴を実現させる構成が経路情報生成部121である。

[0208] 以下の説明において、コンテンツ鍵mekをセット鍵k(S_0)で暗号化した暗号文をC(k(S_0)、mek)と表記する。また、部分集合S_i＝[SP_i、TP_i]のSP_i、TP_i、S_iは下記の意味を有する。

[0209] (1)座標点S_iが右向きの有向グラフに含まれる場合

SP_i: 部分集合S_iの要素中で最も小さな番号

TP_i: 部分集合S_iの要素中で最も大きな番号

⇒ $S_i = \{SP_i, SP_{i+1}, \cdots, TP_i\}$

(2)座標点S_iが左向きの有向グラフに含まれる場合

SP_i: 部分集合S_iの要素中で最も大きな番号

TP_i: 部分集合S_iの要素中で最も小さな番号

⇒ $S_i = \{SP_i, SP_{i-1}, \cdots, TP_i\}$

(3)$SP_i = TP_i$の場合

⇒ $S_i = \{SP_i\}$

[0210] なお、SP_iとTP_iは1以上n以下の値である。また、SP_iは有向グラフの始点と交差する縦線の番号(契約者の番号)を表し、TP_iは選択された部分集合の座標点と交差する縦線の番号(契約者の番号)を表す。

[0211] まず、経路情報生成部121は、下式(5)に示すように、上記の部分集合S_iに含まれる契約者の情報に対し、当該部分集合S_iを導出するのに必要な有向パスの情報を生成して付加する。なお、本実施形態に係る経路情報生成部121は、有向パスの情報として、当該有向パスに含まれる各有向枝の終端を表す情報(交差する縦軸の番号IP_{ij};$1 \leqq IP_{ij} \leqq n$)を付加する。但し、有向グラフ上の座標点$[SP_i, SP_i]$と座標点$[SP_i, TP_i]$とを結ぶ有向パスにp本($p \leqq DD_T$)の有向枝が存在するものとする。

[0212] [数5]

$$S_i = (SP_i, IP_{i1}, \cdots, IP_{i(p-1)}, TP_i) \quad \cdots (5)$$

[0213] (例1)

例えば、契約者数n=64、パラメータk=6のAI05方式において、部分集合決定部120が部分集合S=[1, 8]を選択した場合を考える。すると、経路情報生成部121は、有向パスの情報を含む部分集合Sの情報として、S=(1, 2, 4, 8)を生成する(図16の太線(有向パス)を参照)。

[0214] (例2)

他の例として、契約者数n=64、パラメータk=6のAI05方式において、契約者45と契約者55とが排除された場合を考える。このとき、部分集合決定部120が部分集合S_1=[1, 44], S_2=[48, 46], S_3=[49, 54], S_4=[64, 56]を選択したとすると

、経路情報生成部121は、各部分集合に有向パスの情報を付加した下記の情報を生成する(図17の太線(有向パス)を参照)。

S_1＝(1, 2, 4, 8, 16, 32, 40, 44)、

S_2＝(48, 47, 46)、

S_3＝(49, 50, 52, 54)、

S_4＝(64, 63, 61, 57, 56)。

[0215] (例3)

他の例として、契約者数n＝64、パラメータk＝6のA06(A＋B)方式において、契約者45と契約者55とが排除された場合を考える。このとき、部分集合決定部120が部分集合S_1＝[1, 44], S_2＝[48, 46], S_3＝[49, 54], S_4＝[64, 56]を選択したとすると、経路情報生成部121は、各部分集合に有向パスの情報を付加した下記の情報を生成する(図18の太線(有向パス)を参照)。

S_1＝(1, 33, 37, 41, 42, 43, 44)、

S_2＝(48, 47, 46)、

S_3＝(49, 53, 54)、

S_4＝(64, 60, 56)。

[0216] 上記の通り、一つの部分集合について有向パスの情報がp＋1個の番号IP_{ij}により表される。また、p≦DD_Tであり、各番号IP_{ij}を表現するのにlog(n)ビットのメモリ領域を要することから、一つの部分集合を表すのに最大(DD_T＋1)＊log(n)ビットが必要であることが分かる。但し、DD_Tの値は採用する鍵配信方式毎に異なる。例えば、AI05方式ではDD_T＝(2k－1)＊($n^{1/k}$－1)であり、A06(A＋B)方式ではDD_T＝k($n^{1/k}$－1)である。

[0217] (通信部118)

通信部118は、暗号化部116により暗号化されたコンテンツ又はコンテンツ鍵を葉ノードに対応する全ての端末装置122に対して配信する。また、通信部118は、有向グラフIに基づいて所定の中間鍵を端末装置122に対して配信する。このとき、通信部118は、各端末装置122が、自身が含まれる部分集合に対応する中間鍵を全て導出できるように必要最低限の中間鍵を配信する。また、通信部118は、所定の有

向グラフの情報を各端末装置122に対して配信する。さらに、通信部118は、許諾契約者の集合(N＼R)、又は許諾契約者の集合(N＼R＝$S_1 \cup S_2 \cup \cdots \cup S_m$)を構成する部分集合($S_1$, S_2, ・・・, S_m)の情報を各端末装置122に配信する。このとき、通信部118は、経路情報生成部121により付加された有向パスの情報も配信する。

[0218] [端末装置122の構成]

次に、図19を参照しながら、本実施形態に係る端末装置122の構成について説明する。図19は、端末装置122の構成を示す説明図である。

[0219] 図19を参照すると、端末装置122は、主に、通信部124と、判断部126と、鍵生成部128と、復号部130とにより構成される。なお、端末装置122は、上記のユーザに対応している。また、通信部124は、上記の鍵生成経路情報取得部、及び暗号情報取得部の一例である。そして、鍵生成部128は、上記の鍵情報生成部の一例である。さらに、復号部130は、上記の暗号情報復号部の一例である。

[0220] (通信部124)

通信部124は、鍵配信サーバ102から配信された情報を受信する。例えば、通信部124は、鍵配信サーバ102から配信されたコンテンツ、コンテンツ鍵、中間鍵、有向グラフに関する情報、又は許諾契約者に関する情報等を受信する。また、通信部124は、有線又は無線のネットワークに接続された複数の情報源(例えば、鍵配信サーバ102)、又はネットワークを介さずに直接的又は間接的に接続された情報源(例えば、光ディスク装置、磁気ディスク装置、又は携帯型端末装置等の情報メディア)から情報を取得する構成であってもよい。

[0221] (判断部126)

判断部126は、セット鍵に対応する部分集合のいずれかに自身が要素として含まれるか否かを判断する。判断部126は、鍵配信サーバ102の部分集合決定部120により選択された部分集合のいずれかに自身が含まれるか否かを判断する。このとき、判断部126は、鍵配信サーバ102から取得した上記部分集合の情報を参照する。

[0222] (鍵生成部128)

鍵生成部128は、予め配信された中間鍵とPRSGとを利用して所望の中間鍵又はセット鍵を生成する。このとき、鍵生成部128は、鍵配信サーバ102から取得した有

向パスの情報を参照し、当該情報に基づいて所望の中間鍵又はセット鍵を生成する。なお、判断部126により自身が含まれる部分集合が存在しないと判断された場合は、中間鍵又はセット鍵の生成処理を終了する。上記のPRSGは、鍵配信サーバ102が保持するPRSGと実質的に同一であり、所定の有向グラフに基づき、有向枝の始端に対応する中間鍵を入力すると、当該中間鍵に対応するセット鍵と、当該有向枝の終端に対応する中間鍵が出力される。もちろん、一つの座標点から複数の有向枝が伸びている場合は、当該座標点に対応する中間鍵を入力すると各有向枝の終端に対応する複数の中間鍵が得られる。

[0223] (アルゴリズム)

ここで、図20を参照しながら、契約者uの端末装置122による鍵導出アルゴリズムについて説明する。図20は、契約者uの端末装置122が鍵を導出する処理を示した説明図である。なお、この処理は、主に、鍵生成部128により実行される。

[0224] まず、契約者uの端末装置122には、鍵配信サーバ102の部分集合決定部120により選択されたm個の部分集合($S_1, \cdots, S_m$)を表す情報と、経路情報生成部121により部分集合毎に付加された有向パスの情報$S_j = (SP_j, IP_{j,1}, \cdots, IP_{j,(p-1)}, TP_j)$(但し、$j=1, \cdots, m$)とが与えられている。また、判断部126により、自身が部分集合$S_i = [SP_i, TP_i]$に含まれていると判断されたものと仮定する。従って、鍵生成部128は、所望の中間鍵又はセット鍵を生成する処理において、有向パスの情報$S_i = (SP_i, IP_{i,1}, \cdots, IP_{i,(p-1)}, TP_i)$を参照する。以下、図20に示した流れ図に沿って具体的に説明する。

[0225] 図20を参照すると、まず、変数$IP_{i,p}$にTP_iの値を設定する(S402)。次いで、カウンタjを1に初期化する(S404)。次いで、契約者uの端末装置122が部分集合$[SP_i, IP_{i,j}]$に含まれるか否かを判断する(S406)。含まれない場合、カウンタjをインクリメントし(S408)、再びステップS406に戻る。逆に、含まれる場合、変数spにSP_iを設定し、変数epに$IP_{i,j}$を設定する(S410)。このとき、契約者uの端末装置122は、部分集合[sp, ep]に対応する中間鍵t([sp, ep])を予め保持している。

[0226] 次いで、中間鍵t([sp, ep])を変数$t_{current}$に設定する(S412)。次いで、$ep = TP_i$か否かを判断する(S414)。$ep = TP_i$である場合、$t_{current}$をPRSGに入力し、その出力P

RSG($t_{current}$)をλビット毎に区切ったk＋1番目の部分（部分集合[SP_i, TP_i]のセット鍵k([SP_i, TP_i])に該当）を取り出し（S424）、セット鍵の生成処理を終了する。

[0227] 逆に、ep＝TP_iでない場合、変数logd（下式（6）を参照）を計算する（S416）。即ち、logdは、$IP_{i,j}$から$IP_{i,j+1}$への有向枝の長さが$n^{1/k}$の何乗であるかを示す数値である。次いで、カウンタjをインクリメントし（S418）、epに対して$IP_{i,j}$を設定する（S420）。次いで、$t_{current}$をPRSGに入力し、その出力PRSG($t_{current}$)をλビット毎に区切ったlogd＋1番目の部分を新たな$t_{current}$に設定する（S422）。その後、ステップS414に戻る。

[0228] [数6]

$$log\ d = \log_{n^{1/k}} \left| IP_{i,(j+1)} - IP_{i,j} \right| \quad \cdots (6)$$

[0229] （復号部130）

復号部130は、鍵生成部128により生成されたセット鍵を用いてコンテンツ又はコンテンツ鍵を復号する。また、復号部130は、コンテンツ鍵を用いてコンテンツを復号する処理も実行可能である。

[0230] 以上、本実施形態に係る端末装置122の構成について説明した。上記の構成により、端末装置122は、鍵配信サーバ102から取得した有向パスの情報を利用して所望のセット鍵を生成することが可能になる。その結果、端末装置122は、膨大な有向グラフの情報を全て保持又は生成する必要がなくなり、メモリ量及び演算負荷を現実的なレベルまで抑制することが可能になる。

[0231] ＜第2実施形態＞

次に、本発明の第2実施形態に係る鍵提供システムの構成、及び鍵配信に係る具体的な方式について詳細に説明する。但し、上記の第1実施形態と実質的に同一の機能構成を有する構成要素については同一の符号を付することにより詳細な説明を省略する。

[0232] 上記の第1実施形態における鍵提供システム100の特徴は、鍵配信サーバ102から端末装置122に対して提供される有向グラフの情報にあることは既に説明した。特に、有向グラフの情報として、所定の座標点に到達する有向パスに含まれる全ての

有向枝の情報を端末装置122に提供する手段に特徴を有するものである。第1実施形態では、当該有向枝の情報として各有向枝の終端を表す情報を考えたが、所定の座標点に到達可能な経路を端末装置122が認識可能であれば必ずしもこれに限定されるものではない。

[0233] そこで、第2実施形態では、鍵配信サーバ102が備える部分集合決定部120により選択された所定の部分集合$S_i=[SP_i, TP_i]$に対応する座標点S_iに対し、当該座標点S_iに到達する有向パスの情報として、当該有向パスに含まれる各有向枝の長さを表す情報$LD_{i,j}$を端末装置122に提供する手段(経路情報生成部121)について説明する。

[0234] なお、上記の各有向枝の長さLD_{ij}は、ある有向グラフの座標点$[SP_i, SP_i]$から座標点$[SP_i, TP_i]$に到達する有向パス上のj番目に位置する有向枝の長さ$len_{i,j}$に対して、下式(7)により表現される値である。つまり、各有向枝の長さは、$n^{1/k}$の$LD_{i,j}$乗として表現される(但し、$0 \leqq LD_{i,j} < k$である)。

[0235] [数7]

$$LD_{i,j} = \log_{n^{1/k}} len_{i,j} \quad \cdots (7)$$

[0236] そこで、鍵配信サーバ102が備える経路情報生成部121は、各有向枝の長さを表す情報$LD_{i,j}$を用いて、上記の部分集合S_iを下式(8)のように表現する。つまり、経路情報生成部121は、部分集合S_iに関し、下式(8)で表現される有向パスの情報を生成する。もちろん、選択された全ての部分集合S_i(i=1, ・・・, m)について同様に有向パスの情報が生成される。

[0237] [数8]

$$S_i = (SP_i, LD_{i,1}, \cdots, LD_{i,p-1}, LD_{i,p}) \quad \cdots (8)$$

[0238] (例1)

例えば、契約者数n=64、パラメータk=6のAI05方式において、契約者45と契約者55とが排除された場合を考える。このとき、部分集合決定部120が部分集合$S_1=[1, 44]$, $S_2=[48, 46]$, $S_3=[49, 54]$, $S_4=[64, 56]$を選択したとすると、第1

実施形態に係る経路情報生成部121が生成する情報は下記のように表現される(図17を参照)。

[0239] (第1実施形態の場合)

S_1=(1, 2, 4, 8, 16, 32, 40, 44)、

S_2=(48, 47, 46)、

S_3=(49, 50, 52, 54)、

S_4=(64, 63, 61, 57, 56)。

[0240] 一方、上記の第1実施形態と同じ条件の下、第2実施形態に係る経路情報生成部121が有向枝の長さに基づいて生成する情報は下記のように表現される。

[0241] (第2実施形態の場合)

S_1=(1, 0, 1, 2, 3, 4, 3, 2)、

S_2=(48, 0, 0)、

S_3=(49, 0, 1, 1)、

S_4=(64, 0, 1, 2, 0)。

[0242] (例2)

他の例として、契約者数n=64、パラメータk=6のA06(A+B)方式において、契約者45と契約者55とが排除された場合を考える。このとき、部分集合決定部120が部分集合S_1=[1, 44], S_2=[48, 46], S_3=[49, 54], S_4=[64, 56]を選択したとすると、第1実施形態に係る経路情報生成部121が生成する情報は下記のように表現される(図18を参照)。

[0243] (第1実施形態の場合)

S_1=(1, 33, 37, 41, 42, 43, 44)、

S_2=(48, 47, 46)、

S_3=(49, 53, 54)、

S_4=(64, 60, 56)。

[0244] 一方、上記の第1実施形態と同じ条件の下、第2実施形態に係る経路情報生成部121が有向枝の長さに基づいて生成する情報は下記のように表現される。

[0245] (第2実施形態の場合)

$S_1=(1, 5, 2, 2, 0, 0, 0)$、

$S_2=(48, 0, 0)$、

$S_3=(49, 4, 0)$、

$S_4=(64, 2, 2)$。

[0246] 上記の通り、第2実施形態を適用すると、一つの部分集合に関する有向パスの情報は、1つの始点情報SP_i($1 \leqq SP_i \leqq n$)とp個の長さ情報$IP_{i,j}$($0 \leqq IP_{i,j} \leqq k-1$)とにより表現される。また、$p \leqq DD_T$であり、各部分集合は$\log(n)+DD_T*\log(k)$ビットのデータで表される。一方、上記の第1実施形態の場合は、一つの部分集合を表すのに$(DD_T+1)*\log(n)$ビットが必要であった。また、$k \mid \log(n)$であるから、$\log(k) \leqq \log(\log(n)) < \log(n)$となり、$\log(n)+DD_T*\log(k) < (DD_T+1)*\log(n)$という関係が得られる。従って、第2実施形態を適用することにより、上記の第1実施形態を適用するよりも各部分集合S_iを表現するための情報を低減させることができる。その結果、鍵配信サーバ102から端末装置122に対して提供される情報量を低減(通信量の削減又は記録媒体の容量を節約)することが可能になる。

[0247] ところで、部分集合として、$S_i=[3, 3]$等の一人のユーザからなる部分集合が選択された場合に、それをどのように表現するかについて考える。この場合、上記の第1実施形態の方式では$S_i=(3, 3)$と表現される。また、上記の第2実施形態の方式ではいくつかの表現方法が考えられるが、1つの表現方法としては、$S_i=(3)$のようにただひとつの数値で表現する方法が考えられる。他の表現方法としては、特殊記号⊥を用いて、$S_i=(3, \perp)$と表現することもできる。後者の方法を採用すると、ユーザ数が2以上の部分集合において2番目以降が必ず0以上の整数となるため、ユーザ数が1であることを認識することが可能になる。

[0248] (アルゴリズム)

次に、図21を参照しながら、第2実施形態に係る端末装置122により、上記の鍵配信サーバ102から取得した各部分集合の情報を利用して鍵が生成されるアルゴリズムについて説明する。図21は、契約者uの端末装置122が鍵を導出する処理を示した説明図である。なお、この処理は、主に、端末装置122が備える鍵生成部128により実行される。

[0249] まず、契約者uの端末装置122には、鍵配信サーバ102の部分集合決定部120により選択されたm個の部分集合(S_1, ・・・, S_m)を表す情報と、経路情報生成部121により部分集合毎に付加された有向パスの情報S_j＝(SP_j, $LD_{j,1}$, ・・・, $LD_{j,p-1}$, $LD_{j,p}$)(但し、j＝1, ・・・, m)とが与えられている。また、判断部126により、自身が部分集合S_i＝[SP_i, TP_i]に含まれていると判断されたものと仮定する。従って、鍵生成部128は、所望の中間鍵又はセット鍵を生成する処理において、有向パスの情報S_i＝(SP_i, $LD_{i,1}$, ・・・, $LD_{i,p-1}$, $LD_{i,p}$)を参照する。以下、図21に示した流れ図に沿って具体的に説明する。

[0250] 図21を参照すると、まず、変数$IP_{i,0}$にSP_iの値を設定する(S432)。次いで、SP_iの奇数／偶数を判断して、SP_iが奇数であれば変数signに1を設定し、SP_iが偶数であれば－1を設定する(S434)。次いで、カウンタjを1からpまで動かしながら、$IP_{i,j}$(下式(9))を計算する(S436)。ここで、pは、部分集合S_1の表現において、SP_iに続く0以上の整数値の個数を示す。つまり、S_1＝[3, 3]等のようにS_1＝(3)やS_1＝(3, ⊥)と表現されるユーザ数1の部分集合の場合、p＝0となるためS436の処理が実行されない。次いで、カウンタjを0に初期化する(S438)。

[0251] [数9]

$$IP_{i,j} = IP_{i,j-1} + sign * n^{LD_{i,j}/k}$$

・・・(9)

[0252] 次いで、契約者uの端末装置122が部分集合[SP_i, $IP_{i,j}$]に含まれるか否かを判断する(S440)。契約者uの端末装置122が部分集合[SP_i, $IP_{i,j}$]に含まれない場合、カウンタjをインクリメントして再びステップS440に戻る(S442)。逆に、契約者uの端末装置122が部分集合[SP_i, $IP_{i,j}$]に含まれる場合、変数spにSP_iの値を設定し、さらに、変数epに$IP_{i,j}$の値を設定する(S444)。次いで、契約者uの端末装置122が予め保持している中間鍵の中から中間鍵t([sp, ep])を選択して$t_{current}$に設定する(S446)。

[0253] 次いで、変数epが$IP_{i,p}$か否かを判断する(S448)。ep＝$IP_{i,p}$である場合、$t_{current}$をPRSGに入力し、その出力PRSG($t_{current}$)をλビット毎に区切ったk＋1番目の部分(セット鍵k([SP_i, $IP_{i,p}$])に該当)を抽出し(S456)、セット鍵の生成処理を終了する。

逆に、ep＝$IP_{i,p}$でない場合、カウンタjをインクリメントする(S450)。次いで、変数epに$IP_{i,j}$の値を設定する(S452)。次いで、$t_{current}$をPRSGに入力し、その出力PRSG($t_{current}$)をλビット毎に区切った$LD_{i,j}$＋1番目の部分を抽出し、$t_{current}$に設定する(S454)。そして、ステップS448に戻る。

[0254] 以上説明したアルゴリズムを用いて所望の鍵を生成することができる。もちろん、本実施形態に係る鍵生成部128は、これに限定されるものではなく、鍵配信サーバ102から取得した有向パスの情報S_iに含まれる各有向枝の長さを表す情報$LD_{i,j}$から、各有向枝の終端を表す情報$IP_{i,j}$を予め算出し、上記の第1実施形態と同様のアルゴリズムを用いて鍵を算出してもよい。

[0255] [効果]

本発明の各実施形態に係る構成を適用することにより、AI05方式等に代表されるブロードキャストエンクリプション方式において、鍵配信サーバ102により選択された各部分集合に対応するセット鍵を導出する際に、端末装置122が鍵生成に要する有向グラフの情報を予め保持しておく必要がなくなるため、端末装置122のメモリ量に対する負担が低減される。

[0256] 上記の第1実施形態では、端末装置122が鍵生成に要する有向パスの情報として、当該有向パスに含まれる全ての有向枝の終端を示す情報を付加して配信する構成とした。一方、上記の第2実施形態では、端末装置122が鍵生成に要する有向パスの情報として、当該有向パスに含まれる全ての有向枝の長さを示す情報を付加して配信する構成とした。上記の第2実施形態を採用すると、第1実施形態に比べて端末装置122に配信する情報量を低減することが可能になる。

[0257] [鍵提供システム100の応用例]

最後に、図22及び図23を参照しながら、上記の各実施形態に係る鍵提供システム100の応用例について簡単に説明する。

[0258] (応用例1)

まず、鍵提供システム100の一応用例として、放送暗号化システム300の構成について説明する。図21は、放送衛星を用いた放送暗号化システム(Broadcast Encryption System)300の構成を示す説明図である。

[0259] 図22を参照すると、放送暗号化システム300は、主に、衛星放送局302と、管理センタ304と、放送衛星306と、住居308と、受信機310とにより構成される。ここで、放送暗号化システム300は、放送チャンネルを介して暗号化されたデータ(暗号テキスト;Ciphertext)を住居308に設置された受信機310に対して配信するシステムである。但し、放送チャンネルとは、例えば、衛星放送配信チャンネルである。また、暗号テキストとは、例えば、暗号鍵、音声データ、映像データ、又はテキストデータ等を含むコンテンツである。

[0260] まず、衛星放送局302には、放送衛星306を介して暗号テキスト等のデータを送信する管理センタ(Broadcast Trusted Center)304が設置される。管理センタ304は、例えば、暗号化用の鍵を選択したり、データの暗号化、及びデータの配信制御を実行する。つまり、管理センタ304は、上記の各実施形態に係る鍵配信サーバ102の一例である。また、住居308に設置された受信機310は、上記の各実施形態に係る端末装置122の一例である。

[0261] 放送衛星306は、管理センタ304と各住居308に設置された受信機310との間を媒介し、当該受信機310に対して暗号テキスト等のデータを放送する。また、受信機310は、例えば、衛星放送受信機等であり、放送衛星306を介して放送されたデータを受信する。なお、図22に示すように、放送暗号化システム300には複数の受信機310が含まれていてもよく、その場合、管理センタ304は、複数の受信機310から成る受信機グループに対してデータを配信する。このとき、管理センタ304は、認証された受信機310のみがデータを復号できるように放送データを暗号化して配信する。

[0262] 以上、鍵提供システム100の一応用例である放送暗号化システム300について説明した。図22では、衛星放送の例を挙げたが、放送暗号化システム300は、例えば、ケーブルテレビジョンやコンピュータネットワーク等の他の放送チャンネルを利用した暗号化システムに対しても容易に応用することが可能である。

[0263] (応用例2)

次に、鍵提供システム100の他の応用例として、放送暗号化システム400の構成について説明する。図23は、記録媒体を用いた放送暗号化システム400の構成を示

す説明図である。

[0264] 図23を参照すると、放送暗号化システム400は、主に、媒体製造業者402と、管理センタ404と、記録媒体406と、配布仲介者408と、住居412と、受信機414とにより構成される。ここで、放送暗号化システム400における放送チャンネルはデータが記録された記録媒体406である。

[0265] まず、媒体製造業者402には、記録媒体406を利用し、配布仲介者408を介して暗号テキスト等のデータを住居412に提供する管理センタ404が設置されている。但し、管理センタ404は、記録媒体406に暗号テキスト等のデータを記録するだけであり、記録媒体406を用いて間接的に暗号テキスト等のデータを提供する。また、記録媒体406は、例えば、読出専用媒体(例えば、CD－ROM、DVD－ROM等)、又は書換可能媒体(例えば、CD－RW、DVD－RW等)等である。上記の応用例1と同様、管理センタ404は、上記の各実施形態に係る鍵配信サーバ102に相当する。但し、暗号テキスト等のデータを記録媒体に記録して提供する点で若干相違するが、本発明に係る鍵配信サーバは、この応用例のように、実施形態に応じて暗号テキスト等の情報を配信する手段を適宜変更することが可能である。

[0266] 媒体製造業者402は、例えば、小売店等の配布仲介者(Distribution Outlet)408に対して暗号テキスト等のデータが記録された記録媒体406を送付する。次いで、配布仲介者408は、媒体406を各住居412に対して提供する。例えば、配布仲介者408は、記録媒体406を各住居412に対応する個人に対して販売する。この個人は、記録媒体406を住居412に持ち帰り、受信機414を利用して記録媒体406に記録されたデータを再生する。この受信機414は、上記の各実施形態に係る端末装置122の一例であるが、暗号テキスト等のデータを記録媒体を介して取得する点で若干相違する。しかし、本発明に係る端末装置は、この応用例のように、実施形態に応じて暗号テキスト等の情報を取得する手段を適宜変更することが可能である。また、受信機414は、例えば、CDプレーヤ、DVDプレーヤ、又はDVD－RWドライブを備えたコンピュータ等であり、記録媒体406に記録されているデータを読み出して再生することが可能な装置により構成されうる。

[0267] 以上、鍵提供システム100の一応用例である放送暗号化システム400について説

明した。図23では、記録媒体406を介して暗号テキスト等のデータを契約者に提供する手段を例に挙げて説明した。このように、本発明に係る鍵配信サーバ及び端末装置は、実施形態に応じて、各種情報の配布手段に関する構成を変更することが可能である。

[0268] 以上、添付図面を参照しながら本発明の好適な実施形態について説明したが、本発明は係る例に限定されないことは言うまでもない。当業者であれば、請求の範囲に記載された範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

[0269] 例えば、上記の論理二分木は、上から下に枝が広がる構造を有するものと仮定したが、必ずしもこれに限定されず、下から上、左から右、又は右から左に向けて枝が広がるように構成することも可能である。このような配置に関わる変更は、単純に論理二分木を回転して配置することにより実現されるため、当該変更に係るいずれの構成についても実質的に同一の技術的範囲に属するものと言える。また、仮有向グラフ、及び有向グラフを形成する水平座標軸を左右反転させる変更についても同様である。

[0270] さて、上記の各実施形態に係る鍵配信サーバ102は、自身で有向グラフを生成する構成要素を含んでいるが、必ずしもこれに限定されない。例えば、本発明に係る鍵配信サーバ102は、所定の有向グラフに関する情報を取得する取得部を備えていてもよく、この場合、木構造設定部104、座標軸設定部106、仮有向グラフ生成部108、及び有向グラフ生成部110の一部又は全部を備えている必要はない。

[0271] また、上記の各実施形態に係る鍵配信サーバ102は、コンテンツ、コンテンツ鍵、セット鍵、中間鍵、許諾契約者に対応する部分集合の情報、又は有向グラフの情報等を端末装置122に配信する通信部118を備えているが、上記の応用例2にも示した通り、これらの情報を提供するために常にネットワークを利用するとは限らない。例えば、鍵配信サーバ102は、通信部118に代えて、記録媒体に情報を記録するための記録部を備えていてもよい。その場合、端末装置122は、通信部124を備える代わりに、情報が記録された記録媒体を読み込むための読出部を備えていてもよい。

請求の範囲

[1] 複数の端末装置と、これら複数の端末装置に対して情報の暗号化又は復号に用いる鍵情報を提供する鍵提供装置とを備える鍵提供システムであって、

前記鍵提供装置は、

前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を取得する集合関係情報取得部と、

前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出部と、

この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供部と、

を備え、

前記端末装置は、

前記一部の鍵生成経路情報を取得する鍵生成経路情報取得部と、

前記一部の鍵生成経路情報に基づき、前記複数の集合情報の一つに対応する鍵情報から前記複数の集合情報の他の一つに対応する鍵情報を生成する鍵情報生成部と、

を備えることを特徴とする、鍵提供システム。

[2] 複数の端末装置に対して情報の暗号化又は復号に用いる鍵情報を提供する鍵提供装置であって、

前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を取得する集合関係情報取得部と、

前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出部と、

この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末

装置に提供する鍵生成経路情報提供部と、

を備えることを特徴とする、鍵提供装置。

[3] 前記鍵生成経路情報提供部は、ネットワークを介して前記鍵生成経路情報を前記端末装置に送信する通信部を備えることを特徴とする、請求項2に記載の鍵提供装置。

[4] 前記鍵生成経路情報提供部は、前記鍵生成経路情報を前記端末装置に提供するための記録媒体に記録する記録部を備えることを特徴とする、請求項2に記載の鍵提供装置。

[5] 前記複数の集合情報の一つに対応する鍵情報を用いて情報を暗号化する暗号化部と、

暗号化された前記情報を前記端末装置に提供する暗号情報提供部と、

をさらに備えることを特徴とする、請求項2に記載の鍵提供装置。

[6] 前記鍵生成経路情報取得部は、前記集合関係情報として、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報に対応付けられた複数の座標点に対し、当該座標点間を結ぶ有向枝によって形成された有向グラフを取得することを特徴とする、請求項2に記載の鍵提供装置。

[7] 前記鍵生成経路情報抽出部は、前記一部の鍵生成経路情報として、前記端末装置が属する前記集合情報に対応付けられた座標点に到達する前記有向グラフの一部を抽出することを特徴とする、請求項6に記載の鍵提供装置。

[8] 前記鍵生成経路情報抽出部は、前記一部の鍵生成経路情報として、前記有向グラフの一部を構成する有向枝の終端位置を示す情報を抽出することを特徴とする、請求項7に記載の鍵提供装置。

[9] 前記鍵生成経路情報抽出部は、前記一部の鍵生成経路情報として、前記有向グラフの一部を構成する有向枝の長さを示す情報を抽出することを特徴とする、請求項7に記載の鍵提供装置。

[10] 前記座標点S_0に対応する前記鍵情報$k(S_0)$の入力に応じて、前記座標点S_0を始端とする全ての前記有向枝の終端の座標点S_1, ・・・, S_mに対応する前記鍵情報$k(S_1)$, ・・・, $k(S_m)$を生成する鍵情報生成部をさらに備えることを特徴とする、請求項6

に記載の鍵提供装置。

[11] 前記鍵情報は、情報を暗号化又は復号するためのセット鍵kと、当該セット鍵kを生成するための中間鍵tとにより構成され、

前記座標点S_0に対応する前記中間鍵t(S_0)の入力に応じて、前記座標点S_0に対応する前記セット鍵k(S_0)と、前記座標点S_0を始端とする全ての前記有向枝の終端の座標点S_1, ・・・, S_mに対応する前記中間鍵t(S_1), ・・・, t(S_m)とを生成する鍵情報生成部をさらに備えることを特徴とする、請求項6に記載の鍵提供装置。

[12] 複数の端末装置に対して情報の暗号化又は復号に用いる鍵情報を提供する鍵提供装置であって、

前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を生成する集合関係情報生成部と、

前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出部と、

この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供部と、

を備えることを特徴とする、鍵提供装置。

[13] 情報の暗号化又は復号に用いる鍵情報を生成する端末装置であって、

複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報の中から抽出された、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を取得する鍵生成経路情報取得部と、

前記一部の鍵生成経路情報に基づき、前記複数の集合情報の一つに対応する鍵情報から前記複数の集合情報の他の一つに対応する鍵情報を生成する鍵情報生成部と、

を備えることを特徴とする、端末装置。

[14] 前記鍵生成経路情報取得部は、ネットワークを介して前記鍵生成経路情報を受信する通信部を備えることを特徴とする、請求項13に記載の端末装置。

[15] 前記鍵生成経路情報取得部は、前記鍵生成経路情報が記録された記録媒体を取得し、前記記録媒体から前記鍵生成経路情報を読み出す読出部を備えることを特徴とする、請求項13に記載の端末装置。

[16] 前記複数の集合情報の他の一つに対応する鍵情報を用いて暗号化された情報を取得する暗号情報取得部と、

前記鍵情報生成部により生成された前記複数の集合情報の他の一つに対応する鍵情報を用いて、前記暗号化された情報を復号する暗号情報復号部と、

をさらに備えることを特徴とする、請求項13に記載の端末装置。

[17] 前記鍵生成経路情報取得部は、前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報に対応付けられた複数の座標点に対し、当該座標点間を結ぶ有向枝によって形成された有向グラフの中から抽出された、前記端末装置が属する前記集合情報に対応付けられた座標点に到達する前記有向グラフの一部を前記一部の鍵生成経路情報として取得することを特徴とする、請求項13に記載の端末装置。

[18] 前記鍵生成経路情報取得部は、前記一部の鍵生成経路情報として、前記有向グラフの一部を構成する有向枝の終端位置を示す情報を取得することを特徴とする、請求項17に記載の端末装置。

[19] 前記鍵生成経路情報取得部は、前記一部の鍵生成経路情報として、前記有向グラフの一部を構成する有向枝の長さを示す情報を取得することを特徴とする、請求項17に記載の端末装置。

[20] 前記有向枝の始端S_0に対応する前記鍵情報$k(S_0)$の入力に応じて、前記有向枝の終端の座標点S_1に対応する前記鍵情報$k(S_1)$を生成する鍵情報生成部をさらに備えることを特徴とする、請求項17に記載の端末装置。

[21] 前記鍵情報は、情報を暗号化又は復号するためのセット鍵kと、当該セット鍵kを生成するための中間鍵tとにより構成され、

前記有向枝の始端S_0に対応する前記中間鍵$t(S_0)$の入力に応じて、前記有向枝

の始端S_0に対応する前記セット鍵$k(S_0)$と、前記有向枝の終端S_1に対応する前記中間鍵$t(S_1)$とを生成する鍵情報生成部をさらに備えることを特徴とする、請求項17に記載の端末装置。

[22] 複数の端末装置に対してデータの暗号化又は復号に用いる鍵情報を提供するための鍵提供方法であって、

前記複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報を取得する集合関係情報取得ステップと、

前記集合関係情報に含まれる複数の前記鍵生成経路情報から、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を抽出する鍵生成経路情報抽出ステップと、

この鍵生成経路情報抽出部で抽出された前記一部の鍵生成経路情報を前記端末装置に提供する鍵生成経路情報提供ステップと、

を含むことを特徴とする、鍵提供方法。

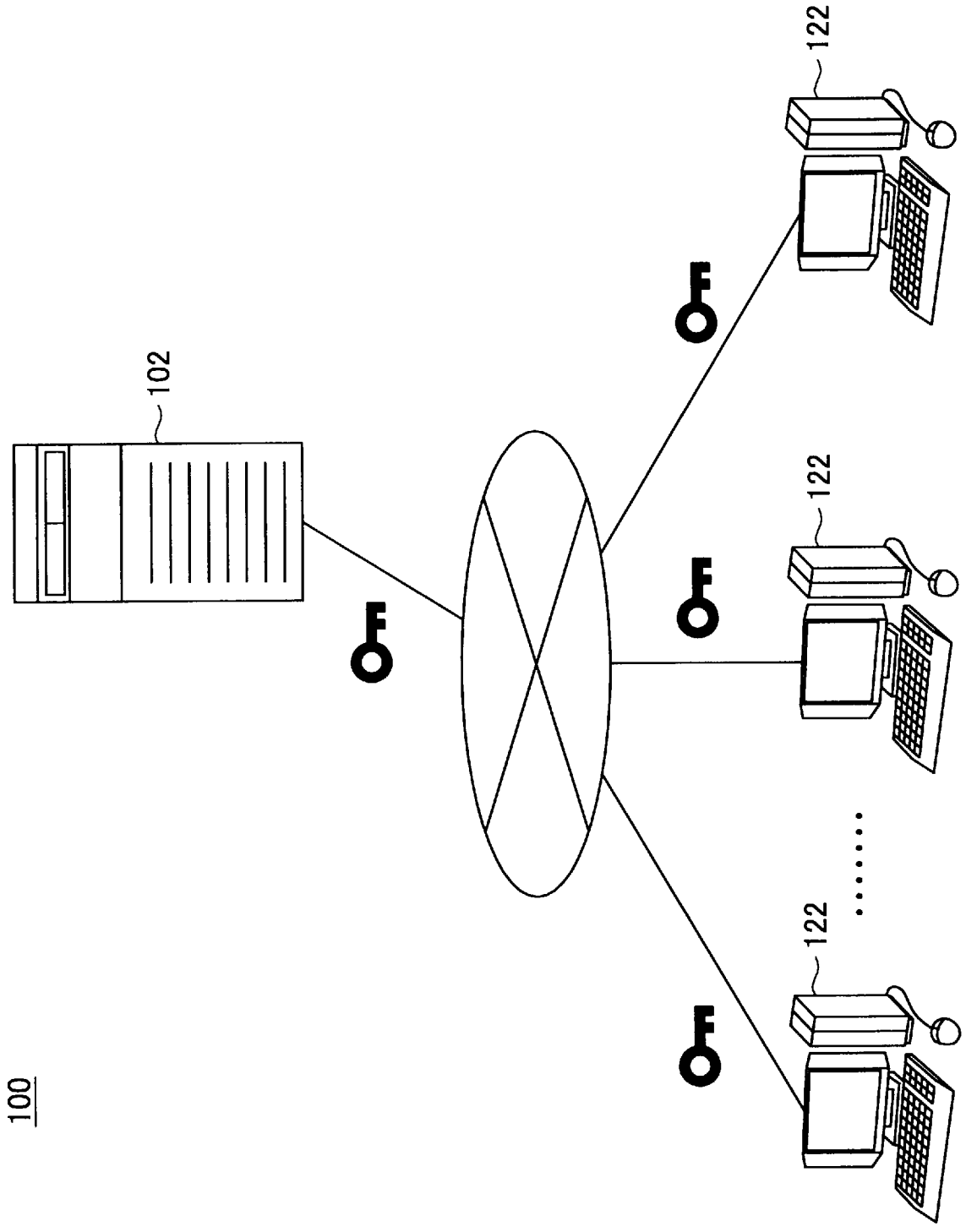
[23] 情報の暗号化又は復号に用いる鍵情報を生成するための鍵生成方法であって、

複数の端末装置の異なる組合せをそれぞれ示す複数の集合情報及びこれら複数の集合情報の一つに対応する鍵情報から他の一つに対応する鍵情報を生成するのに必要となる鍵生成経路を示す鍵生成経路情報を複数含む集合関係情報の中から抽出された、これら複数の前記鍵生成経路情報の一部の鍵生成経路情報を取得する鍵生成経路情報取得ステップと、

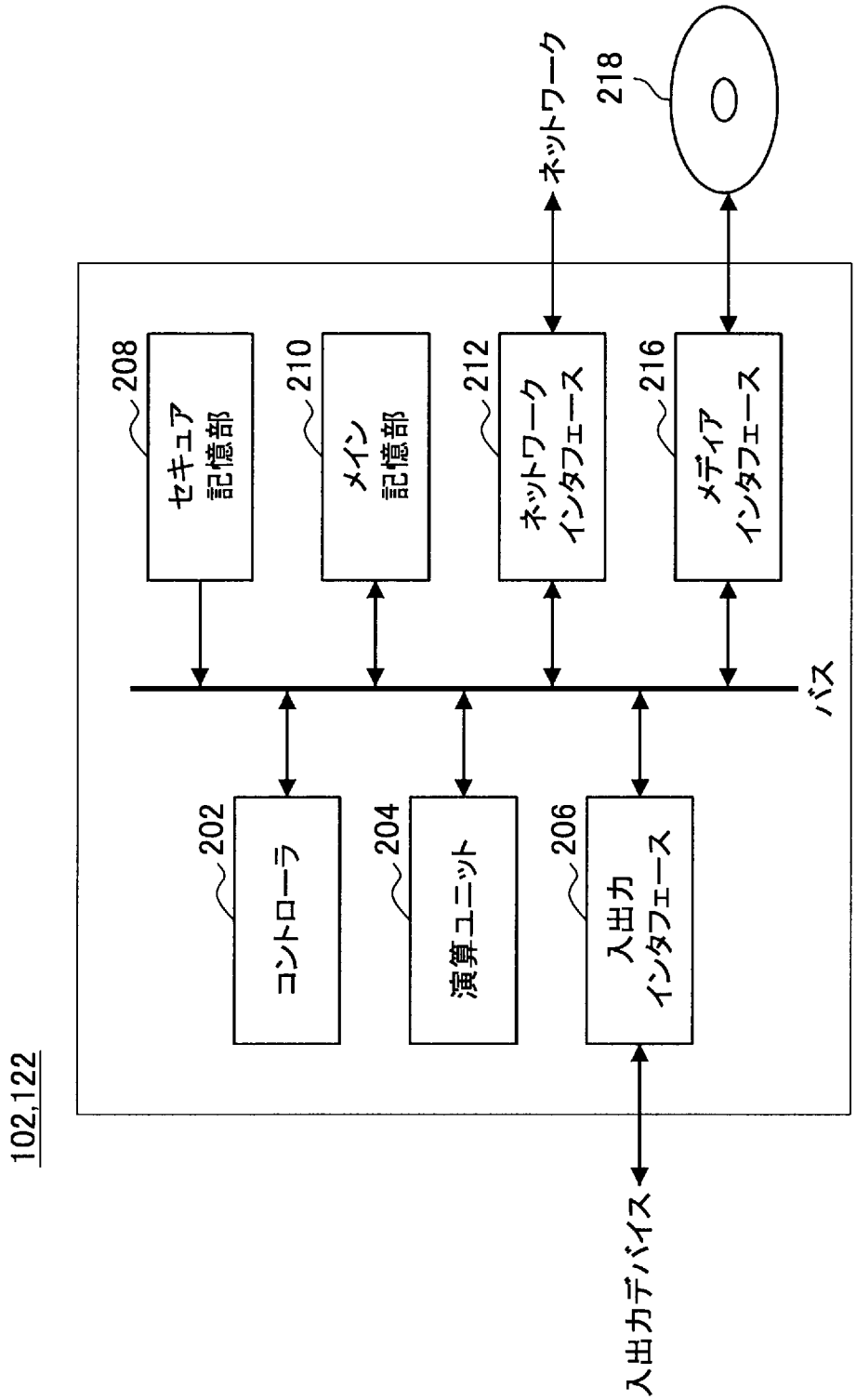
前記一部の鍵生成経路情報に基づき、前記複数の集合情報の一つに対応する鍵情報から前記複数の集合情報の他の一つに対応する鍵情報を生成する鍵情報生成ステップと、

を含むことを特徴とする、鍵生成方法。

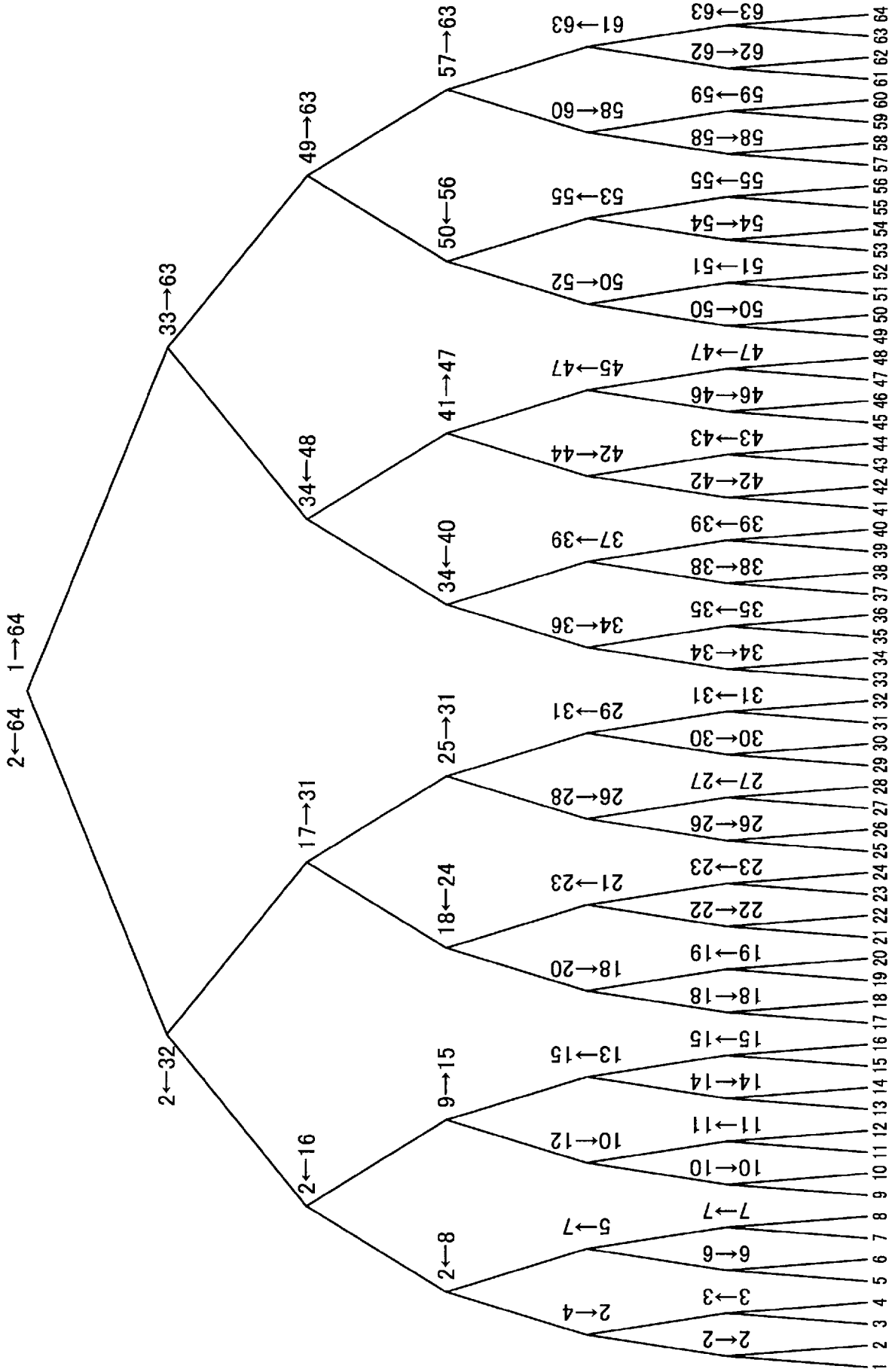
[図1]



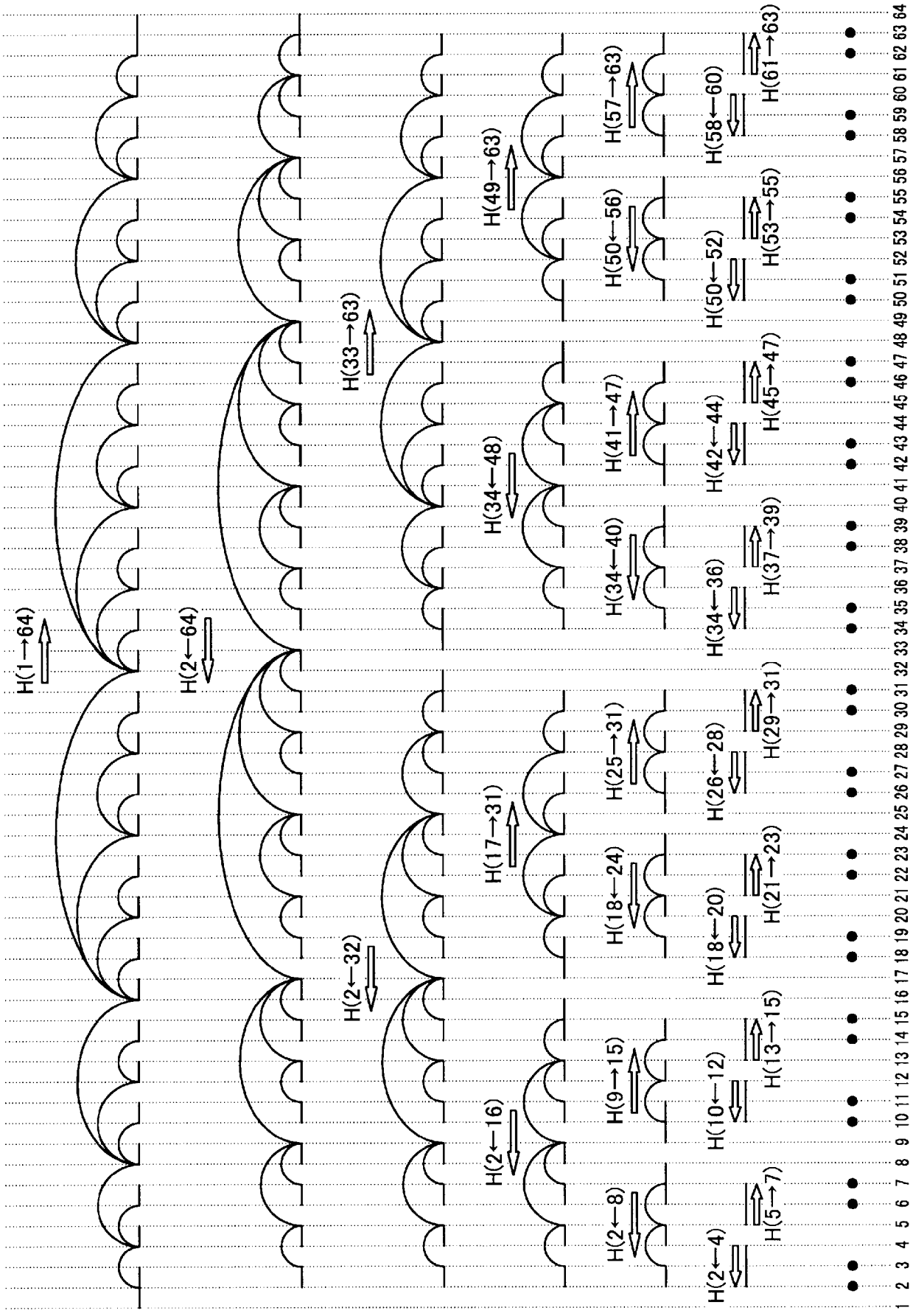
[図2]


102,122
202
コントローラ
204
演算ユニット
206
入出力
インタフェース
208
セキュア
記憶部
210
メイン
記憶部
212
ネットワーク
インタフェース
216
メディア
インタフェース
バス
ネットワーク
218
入出力デバイス

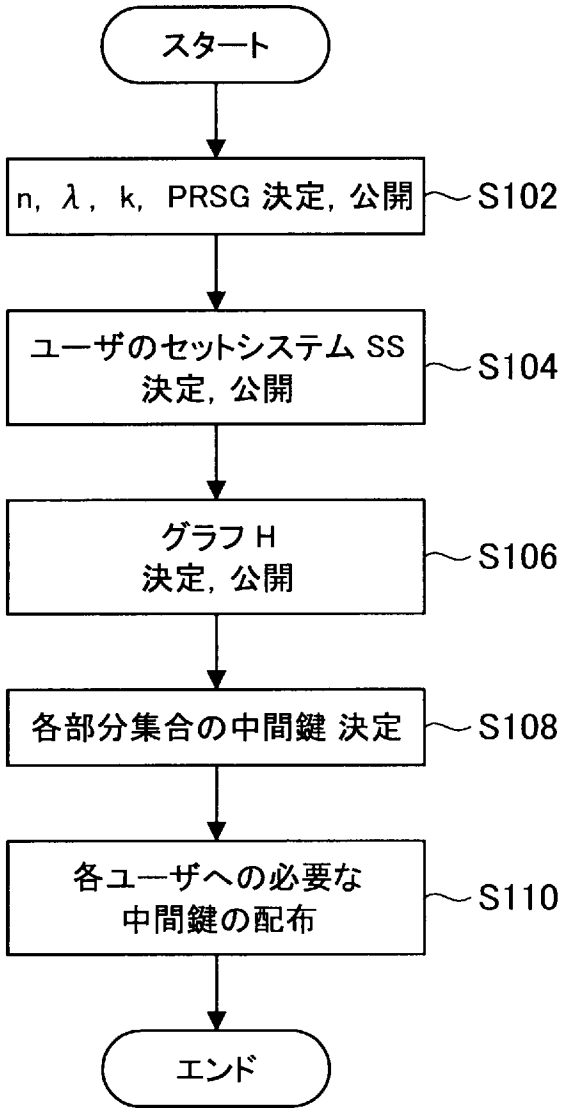
[図3]


1→64
2←64
33→63
2←32
49→63
17→31
34←48
2←16
57→63
25→31
41→47
9→15
50←56
18←24
34←40
2←8
61→63
29→31
45→47
13→15
53→55
21→23
37→39
10→12
58→60
26→28
42→44
5→7
50→52
18→20
34→36
2→4
63→63
31→31
47→47
15→15
55→55
23→23
39→39
11→11
59→59
27→27
43→43
7→7
51→51
19→19
35→35
3→3
62→62
30→30
46→46
14→14
54→54
22→22
38→38
6→6
58→58
26→26
42→42
10→10
50→50
18→18
34→34
2→2
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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

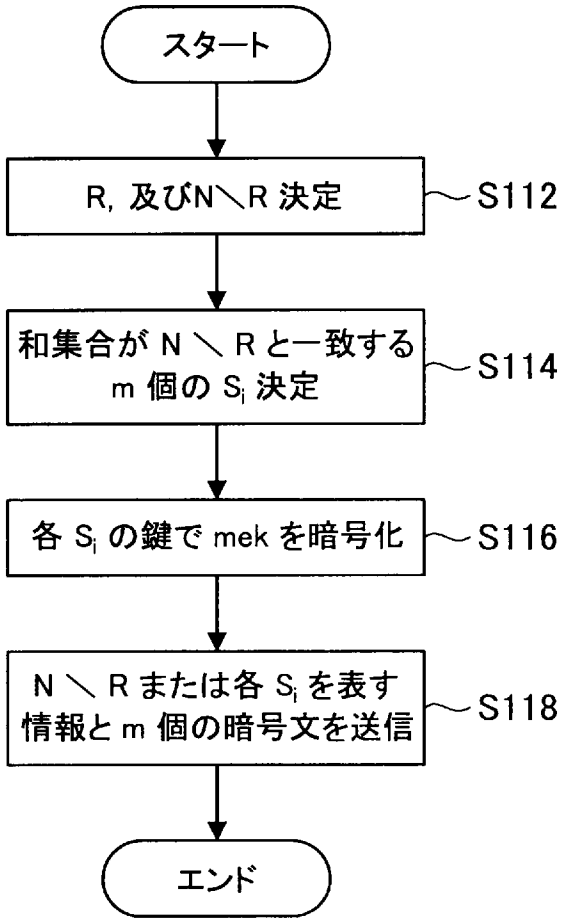
[図4]


H(1→64)
H(2←64)
H(33→63)
H(2←32)
H(49→63)
H(34←48)
H(17→31)
H(2←16)
H(57→63)
H(50←56)
H(41→47)
H(34←40)
H(25→31)
H(18←24)
H(9→15)
H(2←8)
H(61→63)
H(58←60)
H(53→55)
H(50←52)
H(45→47)
H(42←44)
H(37→39)
H(34←36)
H(29→31)
H(26←28)
H(21→23)
H(18←20)
H(13→15)
H(10←12)
H(5→7)
H(2←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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

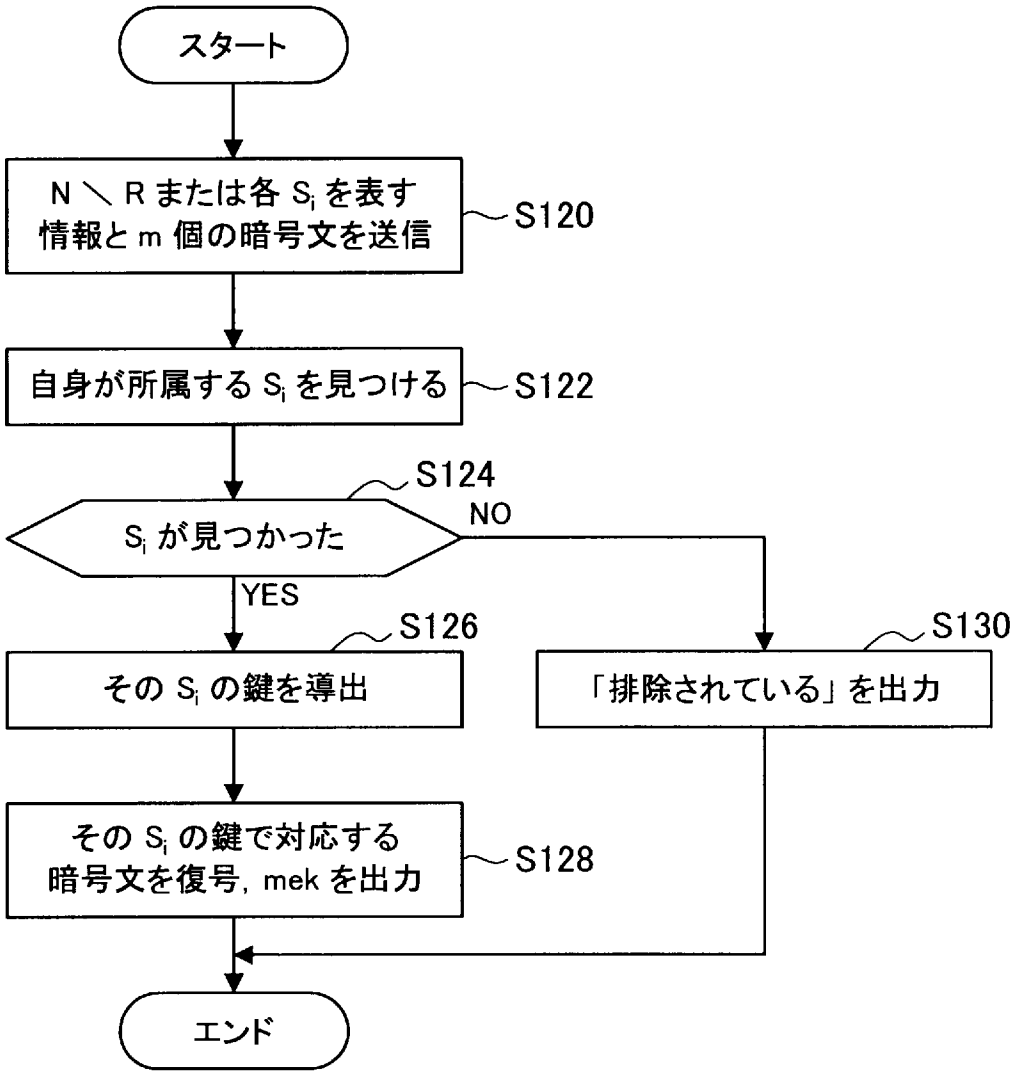
[図5]


スタート
n, λ, k, PRSG 決定, 公開
S102
ユーザのセットシステム SS
決定, 公開
S104
グラフ H
決定, 公開
S106
各部分集合の中間鍵 決定
S108
各ユーザへの必要な
中間鍵の配布
S110
エンド

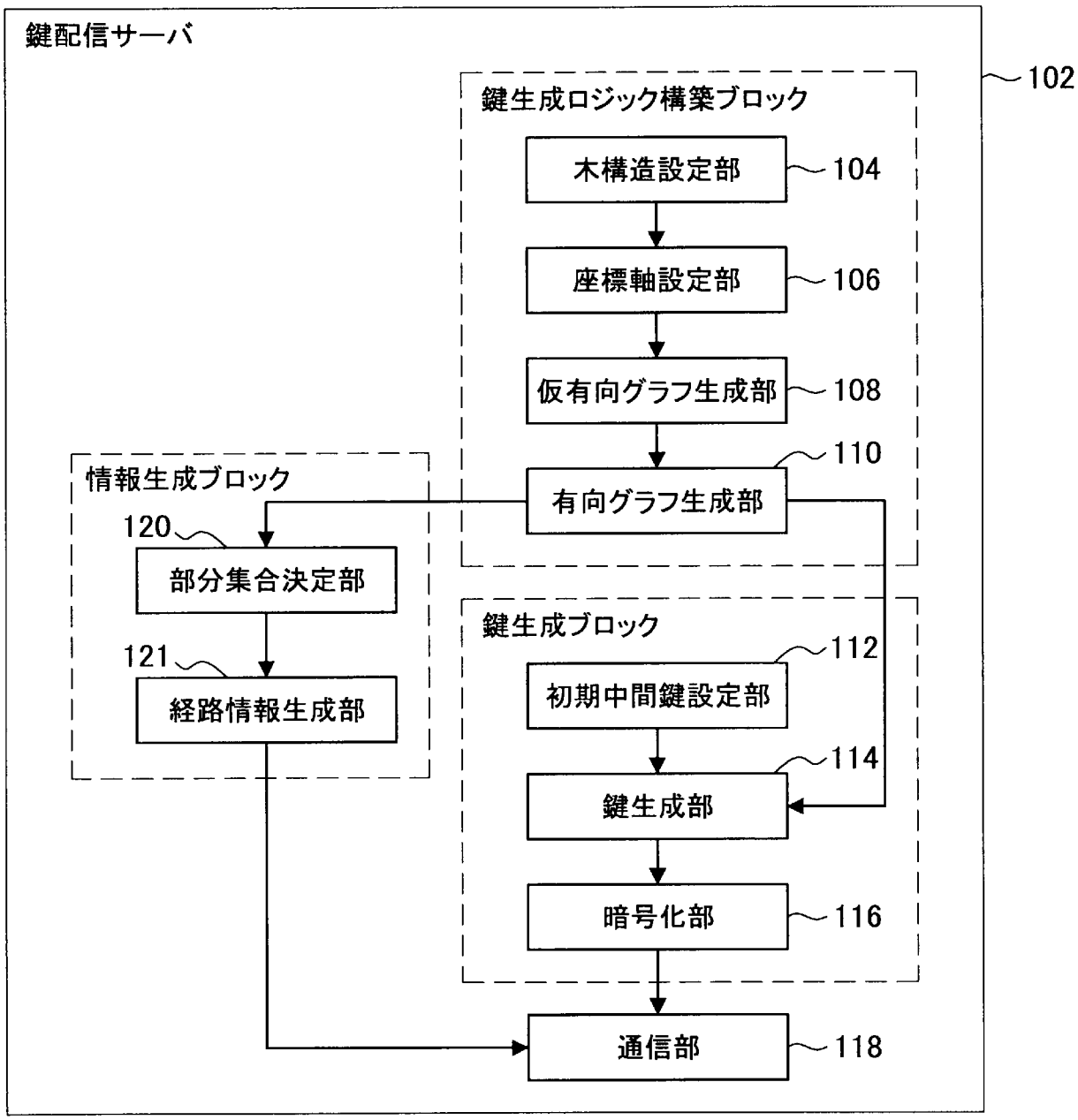
[図6]


スタート
R, 及びN＼R 決定
S112
和集合が N ＼ R と一致する m 個の S_i 決定
S114
各 S_i の鍵で mek を暗号化
S116
N ＼ R または各 S_i を表す情報と m 個の暗号文を送信
S118
エンド

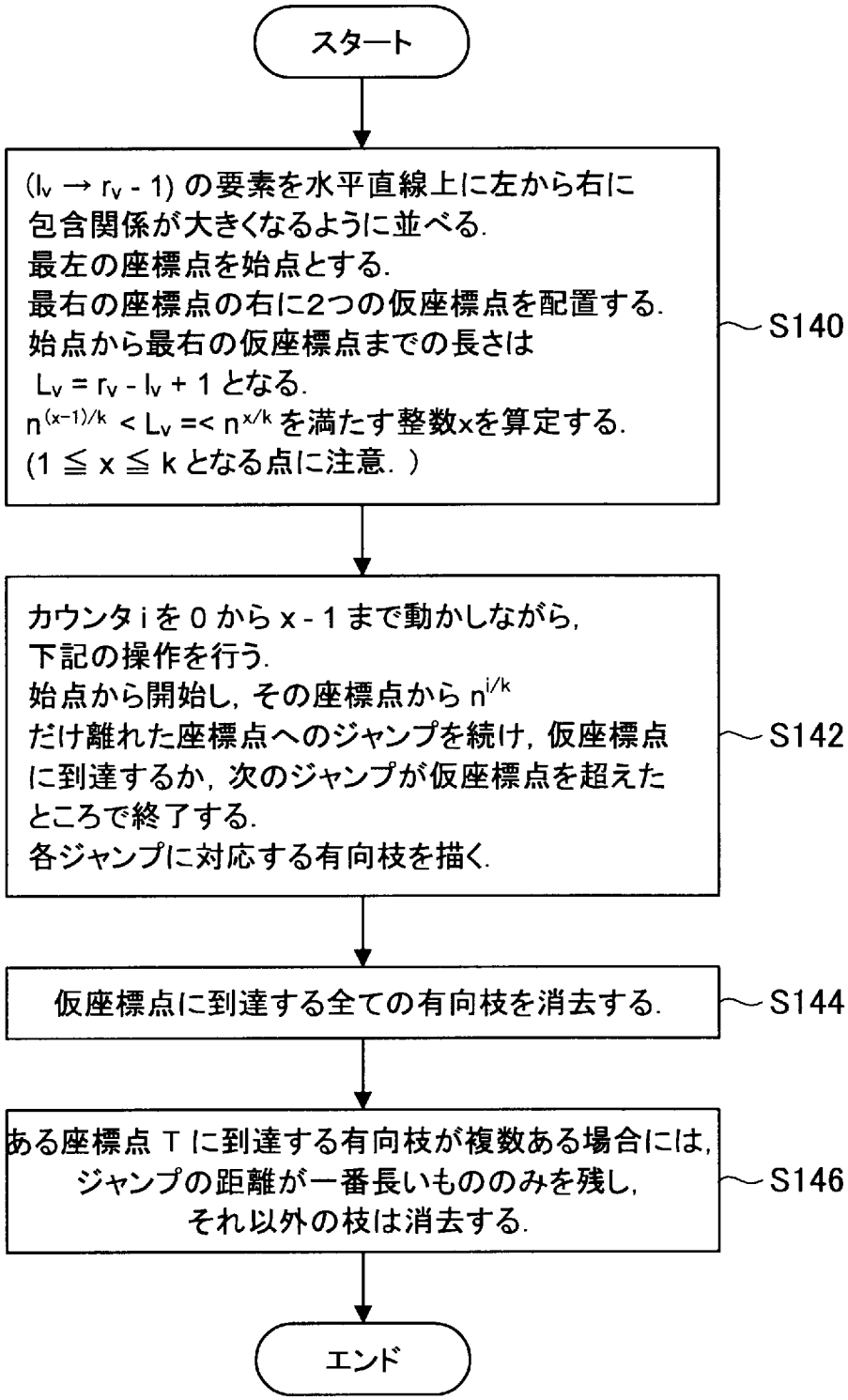
[図7]


スタート
N ＼ R または各 S_i を表す情報と m 個の暗号文を送信
S120
自身が所属する S_i を見つける
S122
S124
S_i が見つかった
NO
YES
S126
その S_i の鍵を導出
S130
「排除されている」を出力
その S_i の鍵で対応する暗号文を復号，mek を出力
S128
エンド

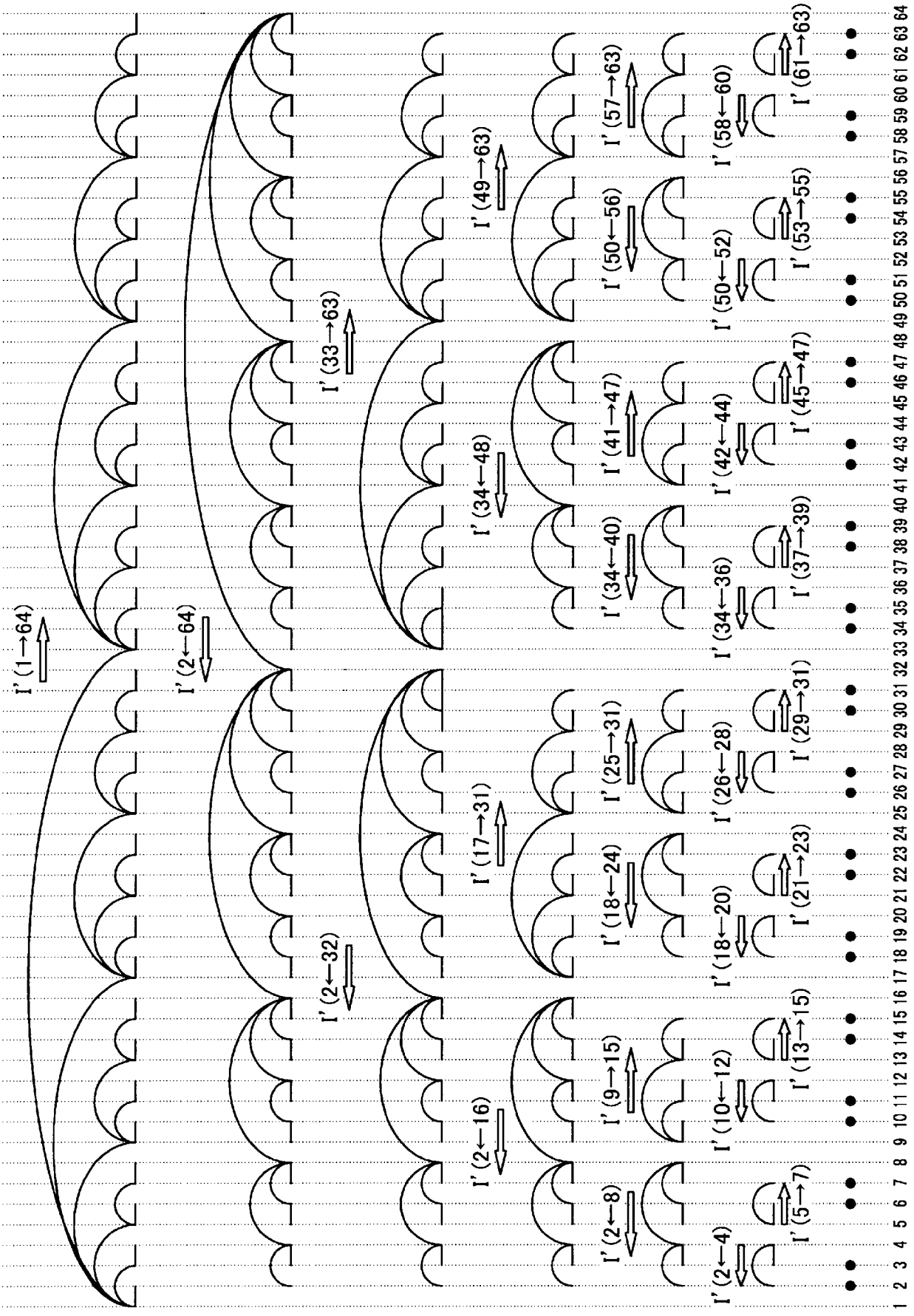
[図8]


鍵配信サーバ
102
鍵生成ロジック構築ブロック
木構造設定部
104
座標軸設定部
106
仮有向グラフ生成部
108
110
有向グラフ生成部
情報生成ブロック
120
部分集合決定部
121
経路情報生成部
鍵生成ブロック
112
初期中間鍵設定部
114
鍵生成部
暗号化部
116
通信部
118

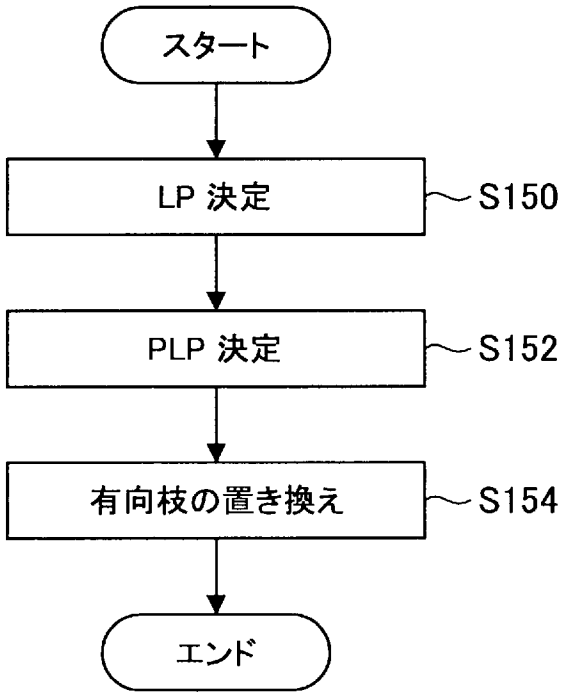
[図9]


スタート
$(l_v \rightarrow r_v - 1)$ の要素を水平直線上に左から右に
包含関係が大きくなるように並べる.
最左の座標点を始点とする.
最右の座標点の右に2つの仮座標点を配置する.
始点から最右の仮座標点までの長さは
$L_v = r_v - l_v + 1$ となる.
$n^{(x-1)/k} < L_v =< n^{x/k}$ を満たす整数xを算定する.
$(1 \leqq x \leqq k$ となる点に注意.)
S140
カウンタ i を 0 から x - 1 まで動かしながら,
下記の操作を行う.
始点から開始し, その座標点から $n^{i/k}$
だけ離れた座標点へのジャンプを続け, 仮座標点
に到達するか, 次のジャンプが仮座標点を超えた
ところで終了する.
各ジャンプに対応する有向枝を描く.
S142
仮座標点に到達する全ての有向枝を消去する.
S144
ある座標点 T に到達する有向枝が複数ある場合には,
ジャンプの距離が一番長いもののみを残し,
それ以外の枝は消去する.
S146
エンド

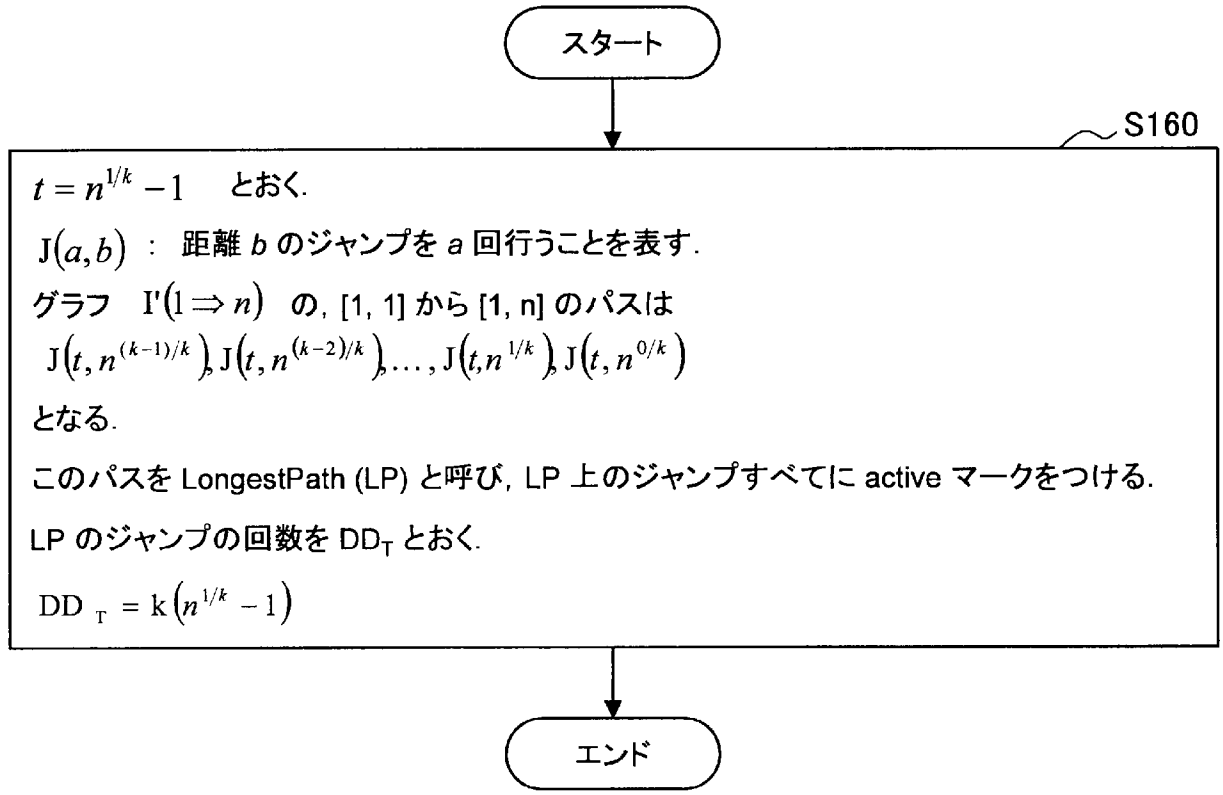
[図10]


I'(1→64)
I'(2←64)
I'(33→63)
I'(2←32)
I'(49→63)
I'(34←48)
I'(17→31)
I'(2←16)
I'(57→63)
I'(50←56)
I'(41→47)
I'(34←40)
I'(25→31)
I'(18←24)
I'(9→15)
I'(2←8)
I'(61→63)
I'(58←60)
I'(53→55)
I'(50←52)
I'(45→47)
I'(42←44)
I'(37→39)
I'(34←36)
I'(29→31)
I'(26←28)
I'(21→23)
I'(18←20)
I'(13→15)
I'(10←12)
I'(5→7)
I'(2←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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

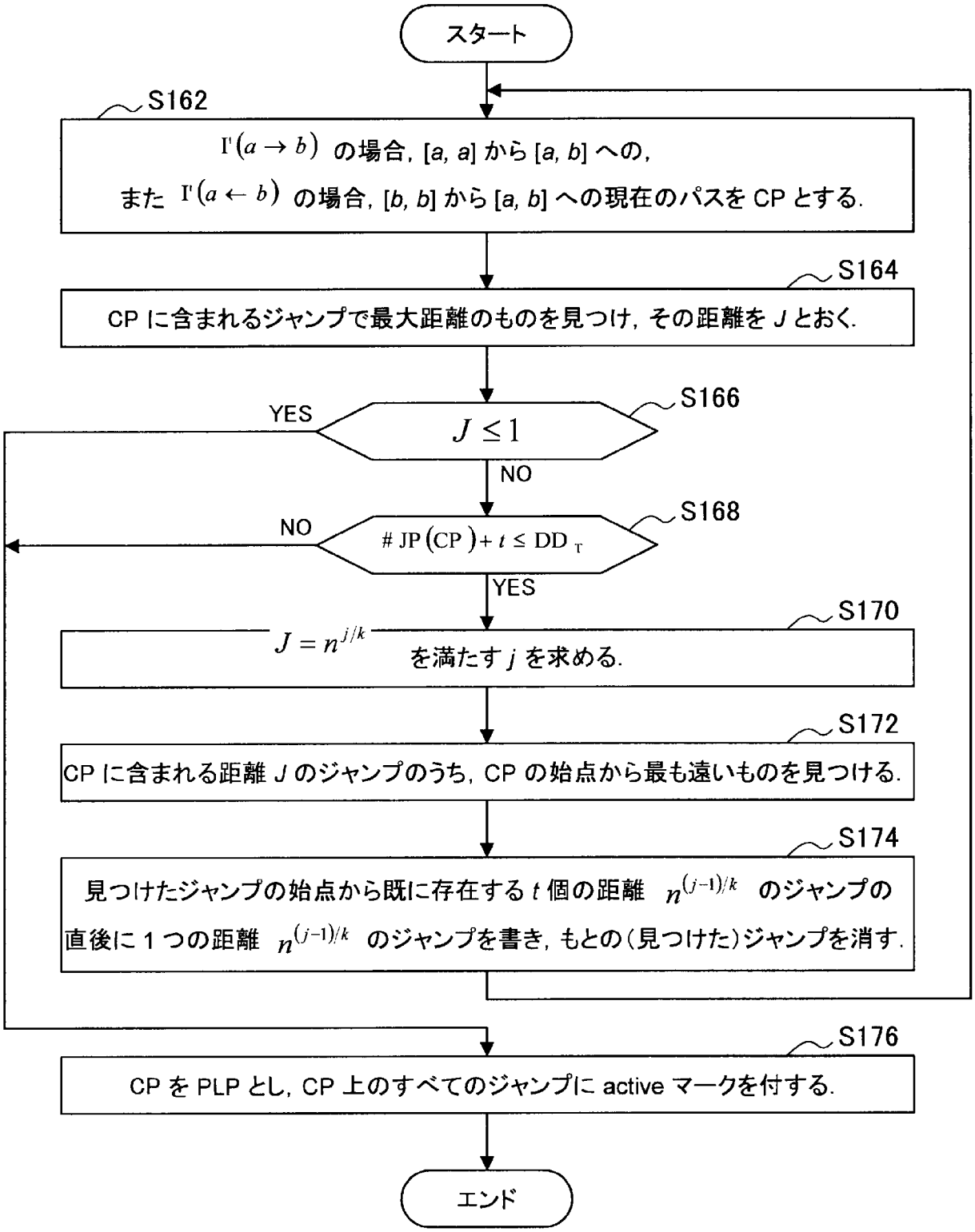
[図11]


スタート
LP 決定
S150
PLP 決定
S152
有向枝の置き換え
S154
エンド

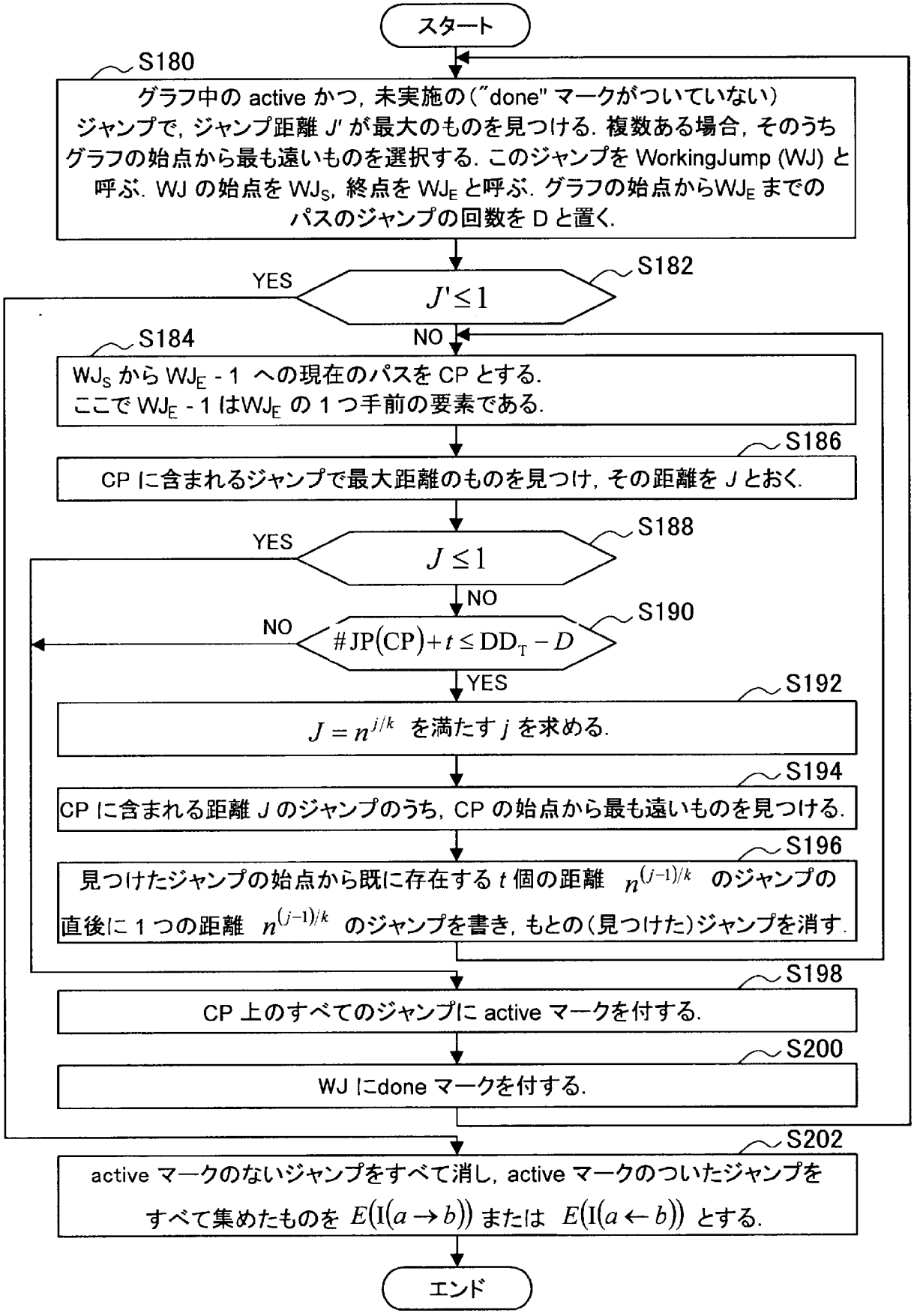
[図12]


スタート
S160
$t = n^{1/k} - 1$ とおく.
$J(a,b)$: 距離 b のジャンプを a 回行うことを表す.
グラフ $I'(1 \Rightarrow n)$ の, [1, 1] から [1, n] のパスは
$J(t, n^{(k-1)/k}), J(t, n^{(k-2)/k}), \ldots, J(t, n^{1/k}), J(t, n^{0/k})$
となる.
このパスを LongestPath (LP) と呼び, LP 上のジャンプすべてに active マークをつける.
LP のジャンプの回数を DD_T とおく.
$DD_T = k(n^{1/k} - 1)$
エンド

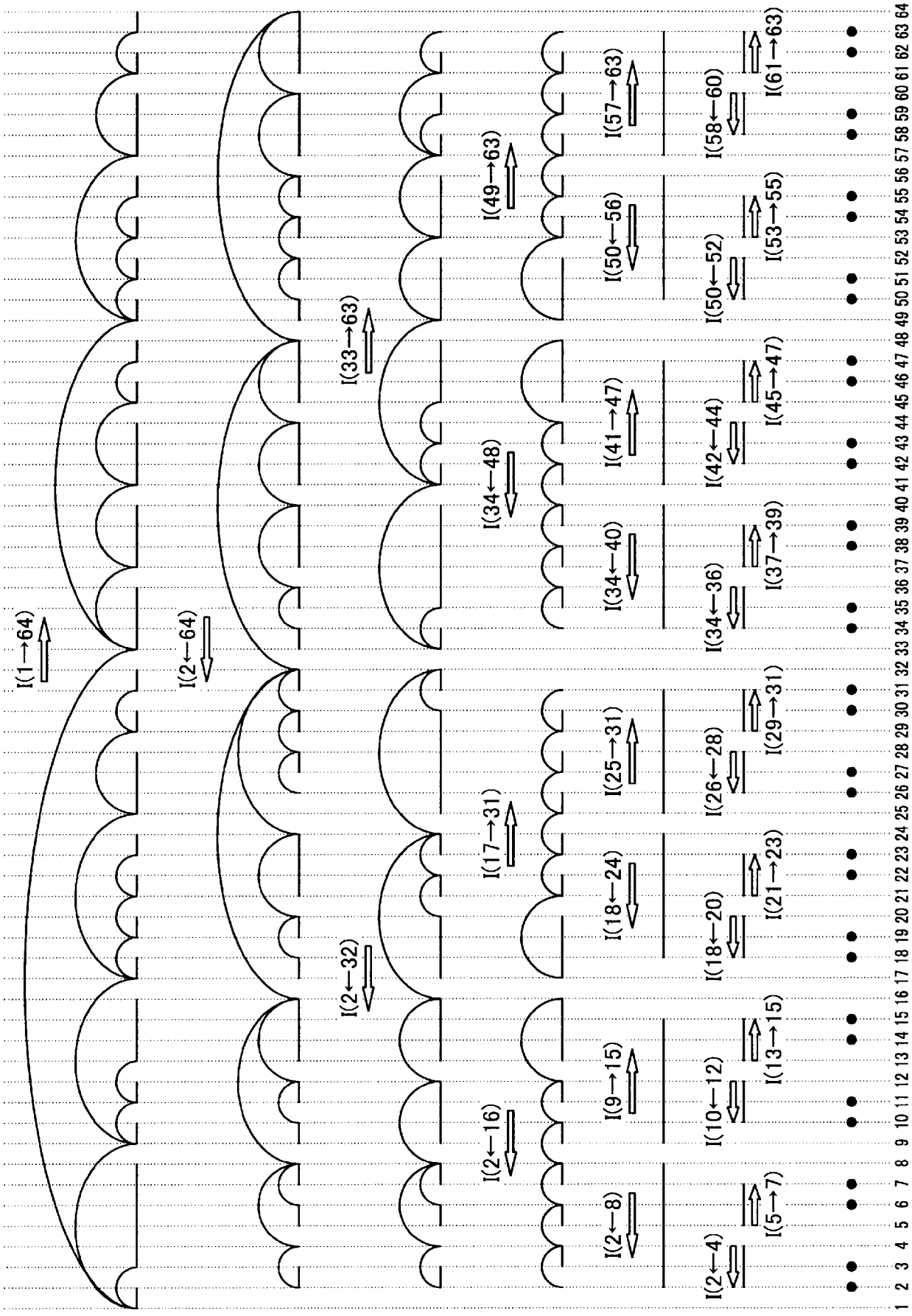
[図13]


スタート
S162
$\Gamma(a \to b)$ の場合，[a, a] から [a, b] への，
また $\Gamma(a \leftarrow b)$ の場合，[b, b] から [a, b] への現在のパスを CP とする．
S164
CP に含まれるジャンプで最大距離のものを見つけ，その距離を J とおく．
S166
YES
$J \leq 1$
NO
S168
NO
$\#\mathrm{JP}(\mathrm{CP}) + t \leq \mathrm{DD}_{\Gamma}$
YES
S170
$J = n^{j/k}$ を満たす j を求める．
S172
CP に含まれる距離 J のジャンプのうち，CP の始点から最も遠いものを見つける．
S174
見つけたジャンプの始点から既に存在する t 個の距離 $n^{(j-1)/k}$ のジャンプの
直後に 1 つの距離 $n^{(j-1)/k}$ のジャンプを書き，もとの（見つけた）ジャンプを消す．
S176
CP を PLP とし，CP 上のすべてのジャンプに active マークを付する．
エンド

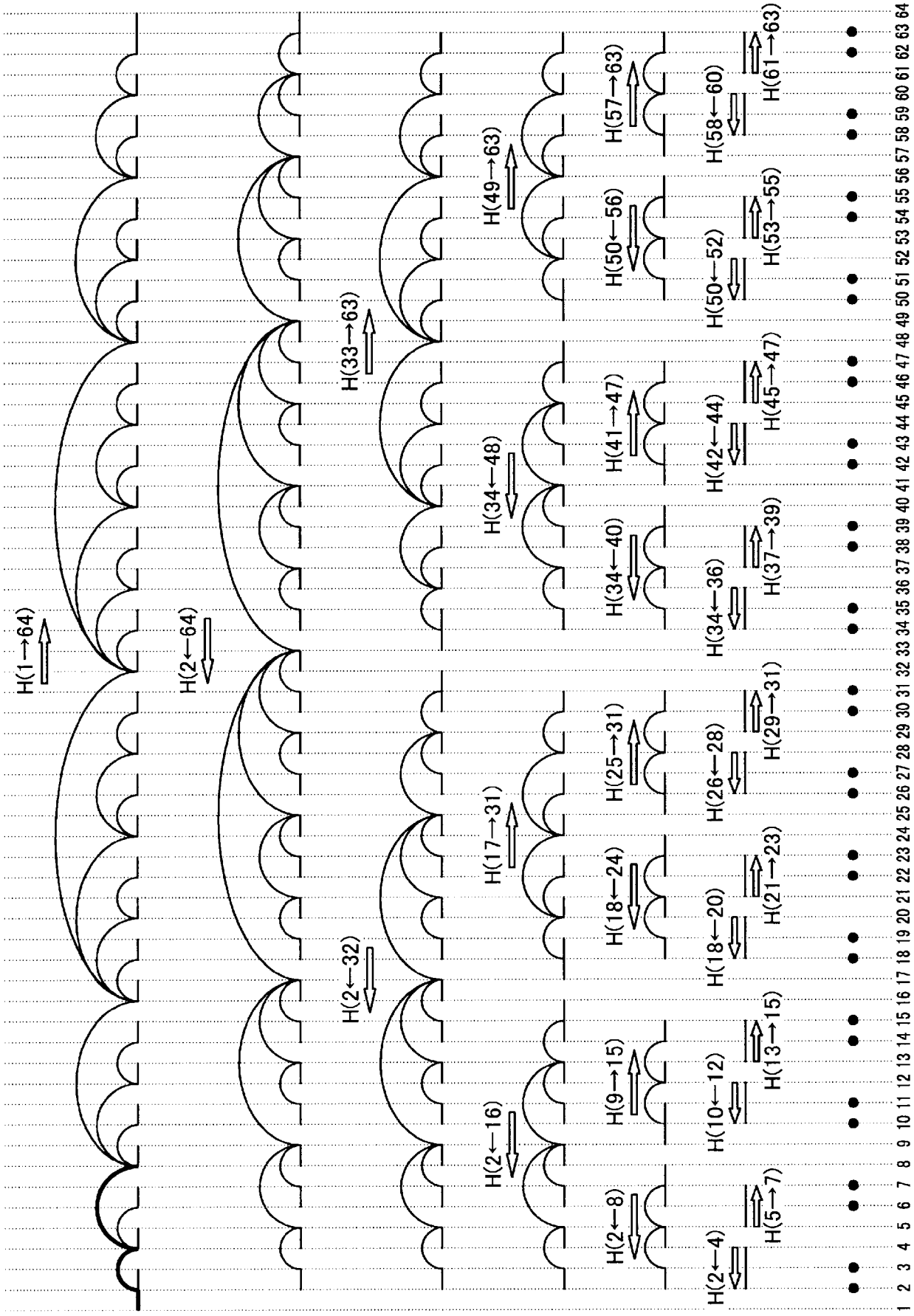
[図14]


スタート
S180
グラフ中の active かつ，未実施の（"done" マークがついていない）ジャンプで，ジャンプ距離 J' が最大のものを見つける．複数ある場合，そのうちグラフの始点から最も遠いものを選択する．このジャンプを WorkingJump (WJ) と呼ぶ．WJ の始点を WJ_S，終点を WJ_E と呼ぶ．グラフの始点からWJ_E までのパスのジャンプの回数を D と置く．
S182
YES
$J' \leq 1$
NO
S184
WJ_S から WJ_E - 1 への現在のパスを CP とする．
ここで WJ_E - 1 はWJ_E の 1 つ手前の要素である．
S186
CP に含まれるジャンプで最大距離のものを見つけ，その距離を J とおく．
S188
YES
$J \leq 1$
NO
S190
NO
$\#\mathrm{JP}(\mathrm{CP}) + t \leq \mathrm{DD}_T - D$
YES
S192
$J = n^{j/k}$ を満たす j を求める．
S194
CP に含まれる距離 J のジャンプのうち，CP の始点から最も遠いものを見つける．
S196
見つけたジャンプの始点から既に存在する t 個の距離 $n^{(j-1)/k}$ のジャンプの直後に 1 つの距離 $n^{(j-1)/k}$ のジャンプを書き，もとの（見つけた）ジャンプを消す．
S198
CP 上のすべてのジャンプに active マークを付する．
S200
WJ にdone マークを付する．
S202
active マークのないジャンプをすべて消し，active マークのついたジャンプをすべて集めたものを $E(\mathrm{I}(a \rightarrow b))$ または $E(\mathrm{I}(a \leftarrow b))$ とする．
エンド

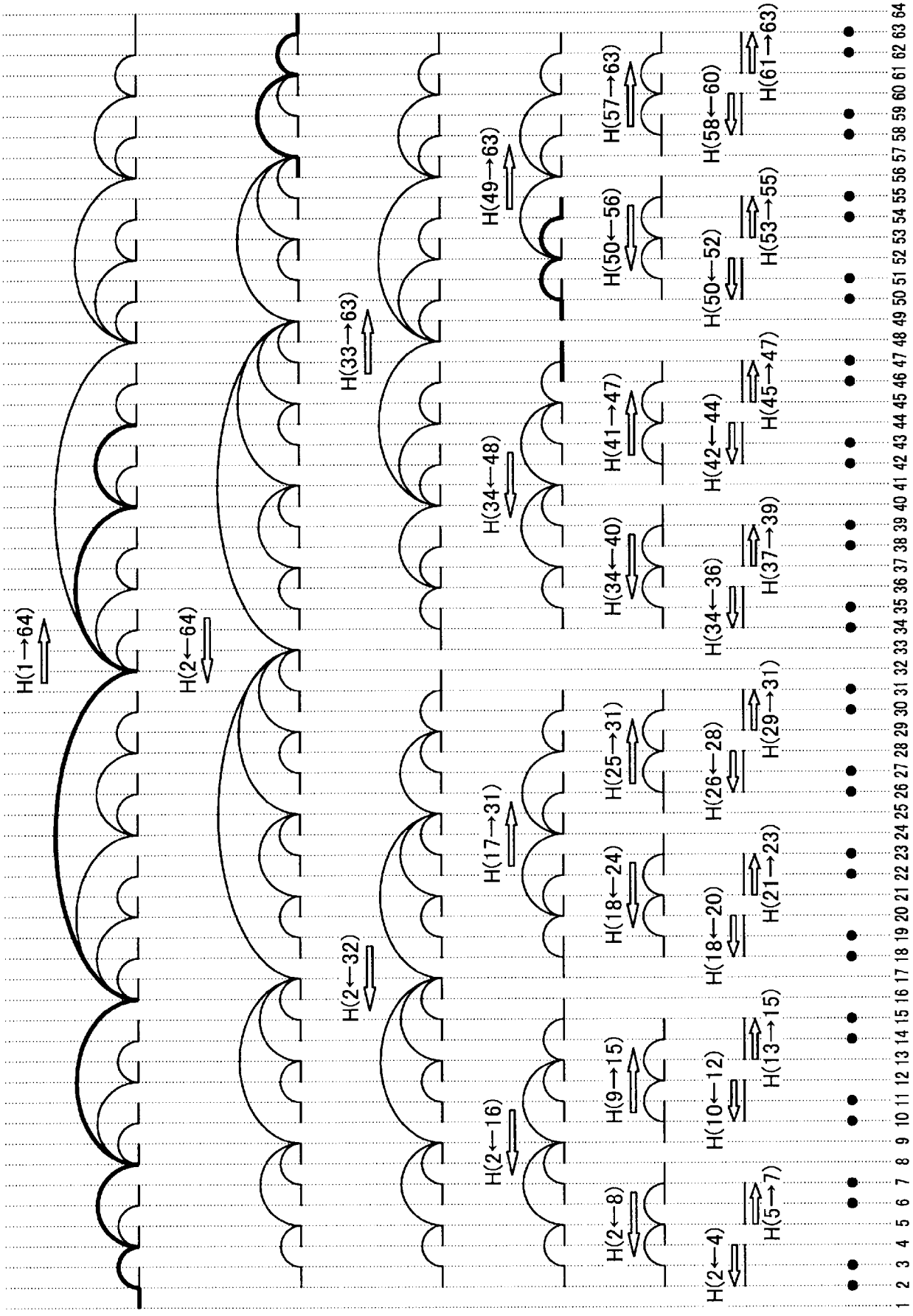
[図15]


I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(49→63)
I(34←48)
I(17→31)
I(57→63)
I(50←56)
I(41→47)
I(2←16)
I(34←40)
I(25→31)
I(61→63)
I(58←60)
I(53→55)
I(50←52)
I(45→47)
I(42←44)
I(37→39)
I(34←36)
I(29→31)
I(26←28)
I(21→23)
I(18←20)
I(13→15)
I(10←12)
I(9→15)
I(18←24)
I(5→7)
I(2←8)
I(2←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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

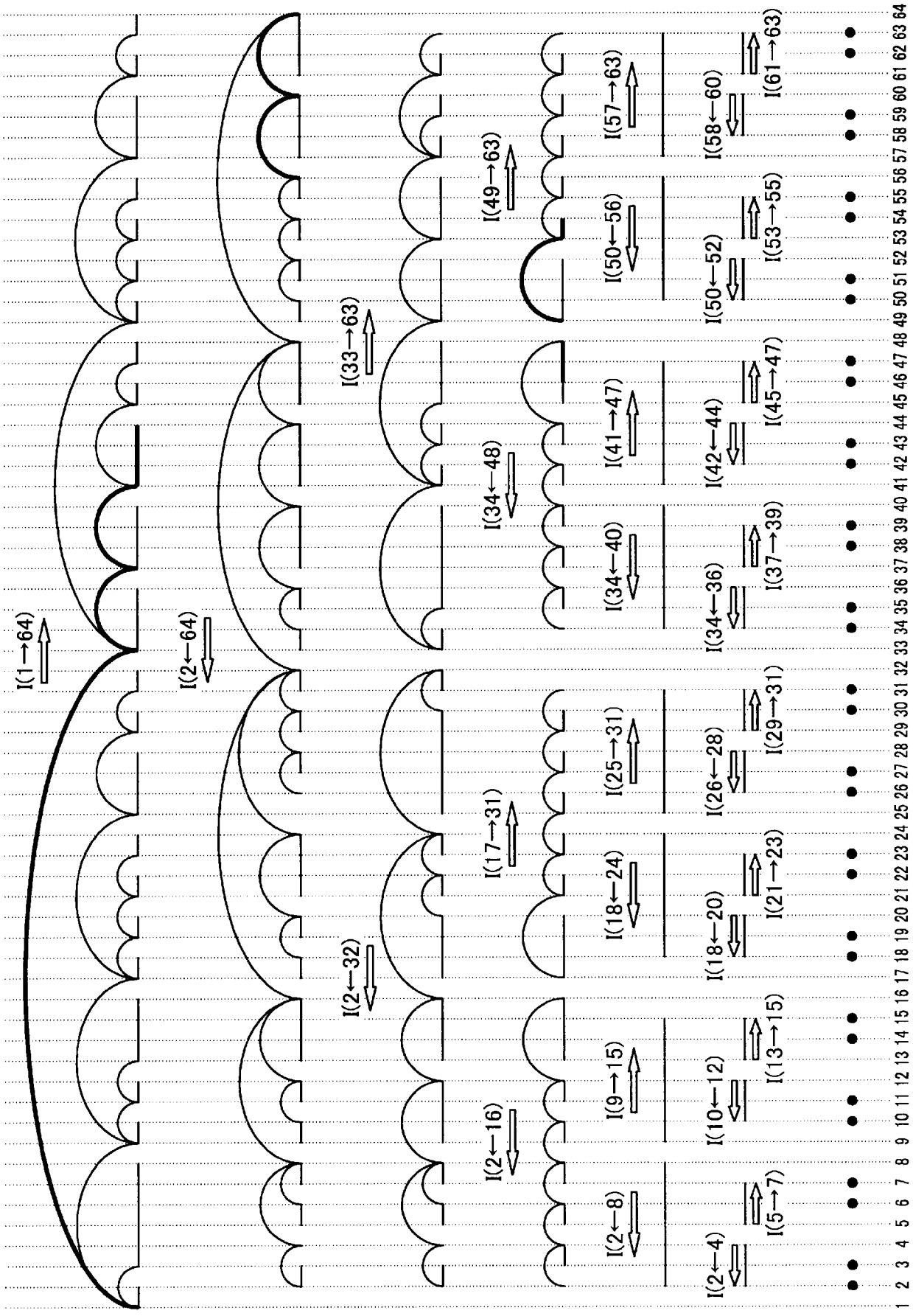
[図16]


H(1→64)
H(2←64)
H(33→63)
H(2←32)
H(49→63)
H(34←48)
H(17→31)
H(2←16)
H(57→63)
H(50←56)
H(41→47)
H(34←40)
H(25→31)
H(18←24)
H(9→15)
H(2←8)
H(61→63)
H(58←60)
H(53→55)
H(50←52)
H(45→47)
H(42←44)
H(37→39)
H(34←36)
H(29→31)
H(26←28)
H(21→23)
H(18←20)
H(13→15)
H(10←12)
H(5→7)
H(2←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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

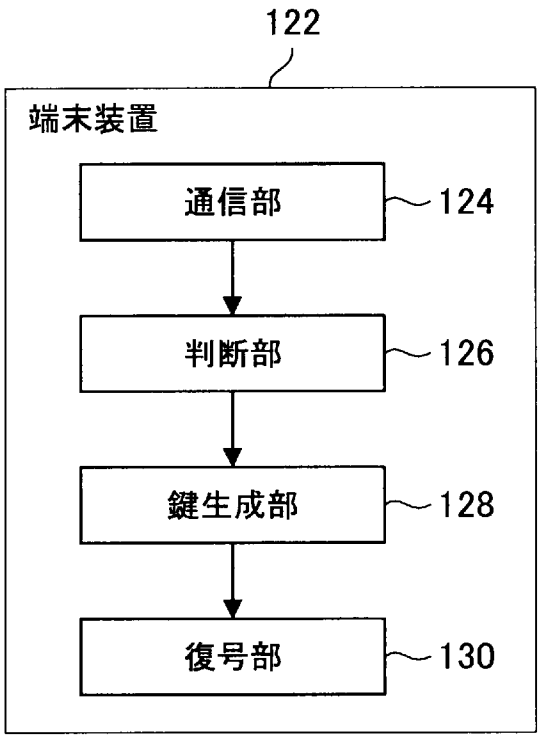
[図17]


H(1→64)
H(2←64)
H(33→63)
H(2←32)
H(49→63)
H(34←48)
H(17→31)
H(2←16)
H(57→63)
H(50←56)
H(41→47)
H(34←40)
H(25→31)
H(18←24)
H(9→15)
H(2←8)
H(61→63)
H(58←60)
H(53→55)
H(50←52)
H(45→47)
H(42←44)
H(37→39)
H(34←36)
H(29→31)
H(26←28)
H(21→23)
H(18←20)
H(13→15)
H(10←12)
H(5→7)
H(2←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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

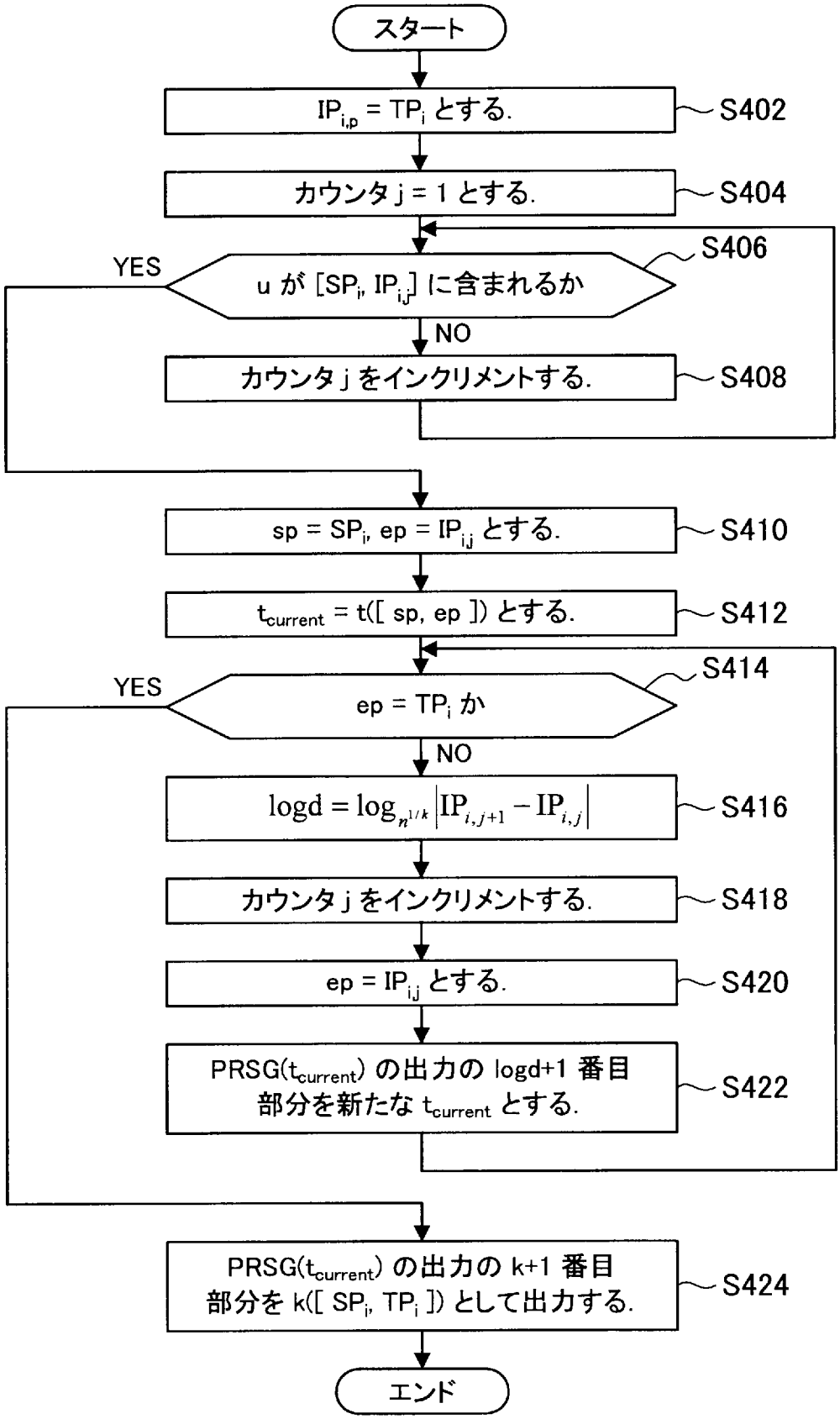
[図18]


I(1→64)
I(2←64)
I(33→63)
I(2←32)
I(49→63)
I(34←48)
I(17→31)
I(2←16)
I(57→63)
I(50←56)
I(41→47)
I(34←40)
I(25→31)
I(18←24)
I(9→15)
I(2←8)
I(61→63)
I(58←60)
I(53→55)
I(50←52)
I(45→47)
I(42←44)
I(37→39)
I(34←36)
I(29→31)
I(26←28)
I(21→23)
I(18←20)
I(13→15)
I(10←12)
I(5→7)
I(2←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 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

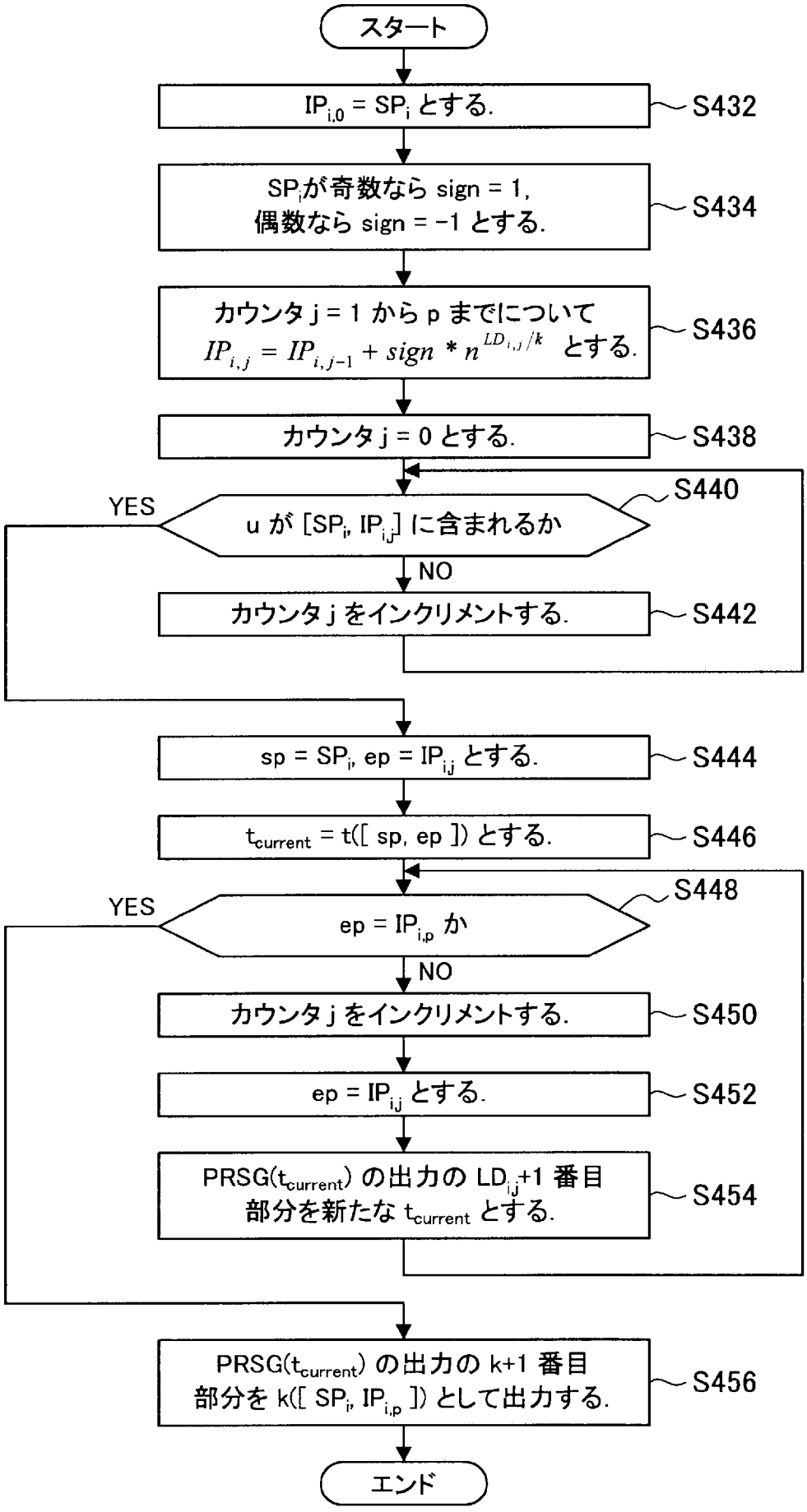
[図19]



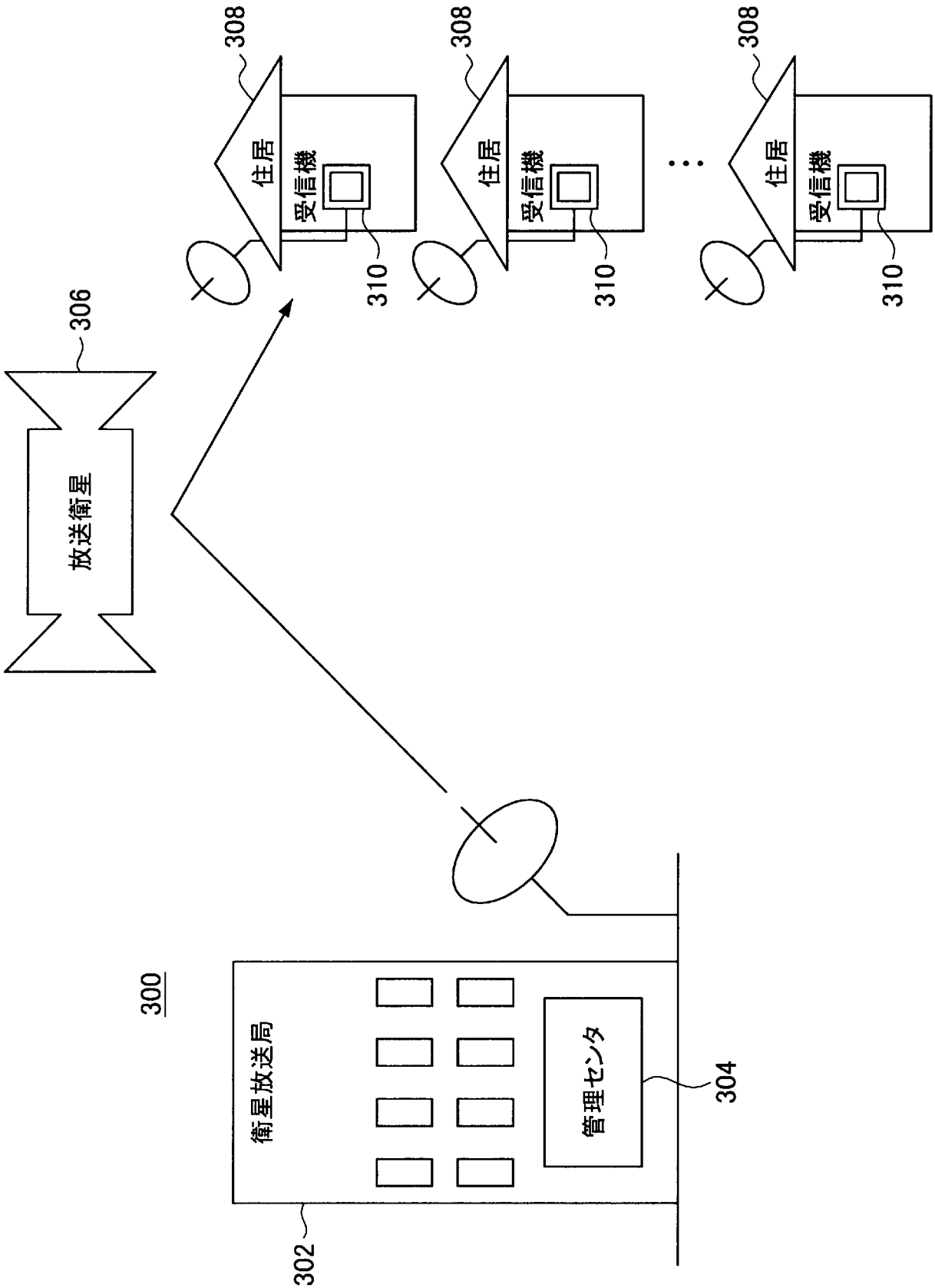
[図20]


スタート
$IP_{i,p} = TP_i$ とする.
S402
カウンタ j = 1 とする.
S404
S406
YES
u が $[SP_i, IP_{i,j}]$ に含まれるか
NO
カウンタ j をインクリメントする.
S408
$sp = SP_i$, $ep = IP_{i,j}$ とする.
S410
$t_{current} = t([\ sp, ep\ ])$ とする.
S412
S414
YES
ep = TP_i か
NO
$\log d = \log_{n^{1/k}} |IP_{i,j+1} - IP_{i,j}|$
S416
カウンタ j をインクリメントする.
S418
$ep = IP_{i,j}$ とする.
S420
PRSG($t_{current}$) の出力の logd+1 番目
部分を新たな $t_{current}$ とする.
S422
PRSG($t_{current}$) の出力の k+1 番目
部分を k([SP_i, TP_i]) として出力する.
S424
エンド

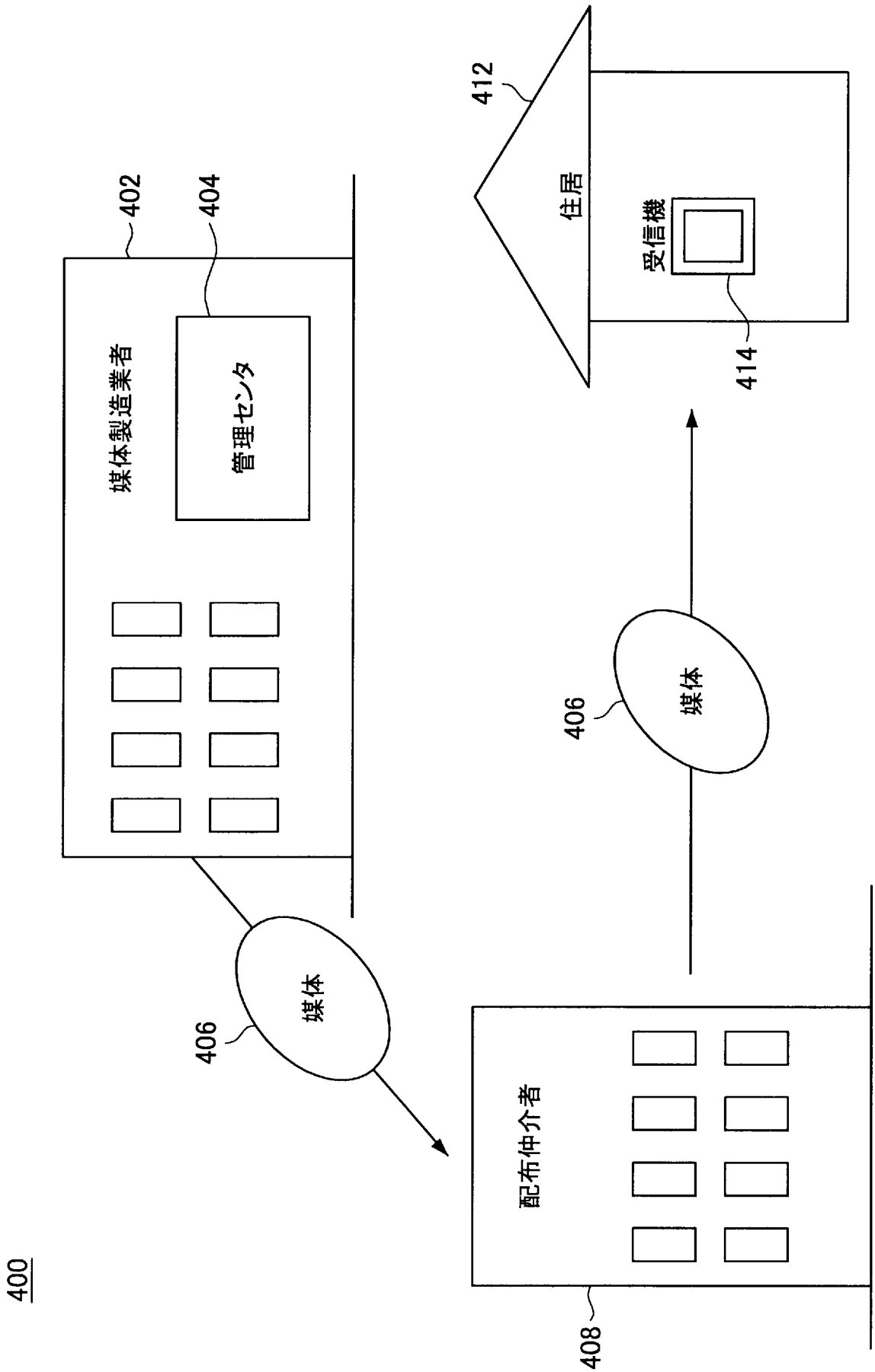
[図21]


スタート
$IP_{i,0} = SP_i$ とする.
S432
SP_iが奇数なら sign = 1,
偶数なら sign = −1 とする.
S434
カウンタ j = 1 から p までについて
$IP_{i,j} = IP_{i,j-1} + sign * n^{LD_{i,j}/k}$ とする.
S436
カウンタ j = 0 とする.
S438
S440
YES
u が $[SP_i, IP_{i,j}]$ に含まれるか
NO
カウンタ j をインクリメントする.
S442
sp = SP_i, ep = $IP_{i,j}$ とする.
S444
$t_{current}$ = t([sp, ep]) とする.
S446
S448
YES
ep = $IP_{i,p}$ か
NO
カウンタ j をインクリメントする.
S450
ep = $IP_{i,j}$ とする.
S452
PRSG($t_{current}$) の出力の $LD_{i,j}$+1 番目
部分を新たな $t_{current}$ とする.
S454
PRSG($t_{current}$) の出力の k+1 番目
部分を k([SP_i, $IP_{i,p}$]) として出力する.
S456
エンド

[図22]



[図23]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/051745

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Nuttapong Attrapadung et.al, "Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext", Dai 28 Kai Symposium on Information Theory and its Applications Yokoshu, No.28, Vol.1, 2005.11.20, p.57-p.60	1-23
Y	JP 2006-74392 A (Canon Inc.), 16 March, 2006 (16.03.06), Par. Nos. [0067] to [0082] & WO 2006/025589 A1	1-23

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 April, 2008 (17.04.08)	01 May, 2008 (01.05.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０５１７４５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	Nuttapong Attrapadung et.al, “Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext”, 第28回情報理論とその応用シンポジウム予稿集, No.28, Vol.1, 2005.11.20, p.57-p.60	1-23
Y	JP 2006-74392 A (キャノン株式会社) 2006.03.16, 【0067】～【0082】段落 & WO 2006/025589 A1	1-23

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 １７．０４．２００８	国際調査報告の発送日 ０１．０５．２００８
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３８５７ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６