(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-182844
(P2012-182844A)
(43)公開日　平成24年9月20日(2012.9.20)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601B	5J104
H04L	9/14	(2006.01)	H04L	9/00	641	

審査請求 有　請求項の数 15　ＯＬ　（全 28 頁）

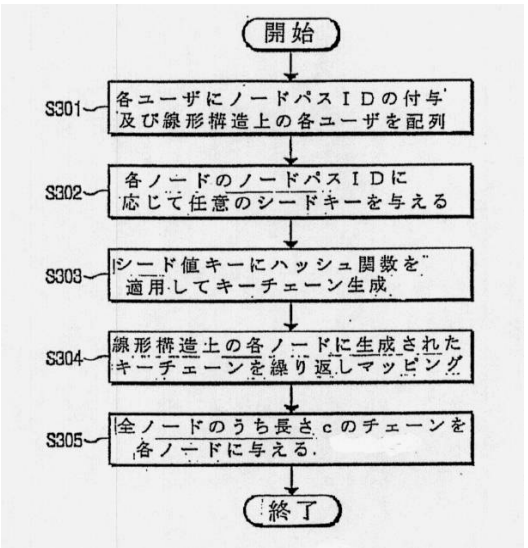
(21)出願番号　特願2012-134570 (P2012-134570)
(22)出願日　平成24年6月14日 (2012.6.14)
(62)分割の表示　特願2011-82596 (P2011-82596)の分割
原出願日　平成17年11月12日 (2005.11.12)
(31)優先権主張番号　10-2004-0092431
(32)優先日　平成16年11月12日 (2004.11.12)
(33)優先権主張国　韓国 (KR)
(31)優先権主張番号　10-2005-0100726
(32)優先日　平成17年10月25日 (2005.10.25)
(33)優先権主張国　韓国 (KR)
(31)優先権主張番号　10-2005-0106604
(32)優先日　平成17年11月8日 (2005.11.8)
(33)優先権主張国　韓国 (KR)

(71)出願人　503447036
サムスン　エレクトロニクス　カンパニー　リミテッド
大韓民国・４４３－７４２・キョンギ－ド・スウォン－シ・ヨントン－ク・サムスン－ロ・１２９
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　デ－ヨプ・キム
大韓民国・ソウル・１５６－８６１・ドンジャク－グ・ヘゥクソク・１－ドン・２０４－１１８

最終頁に続く

(54)【発明の名称】ブロードキャスト暗号化のためのユーザキー管理方法

(57)【要約】
【課題】線形構造を使用して各ノード別に順次一方向キーチェーンを形成し、キー値を分配するブロードキャスト暗号化のためのユーザキー管理方法を提供する。
【解決手段】本発明のキー管理方法は、順次配列された各ノードにノードパスＩＤ（Ｎｏｄｅ　Ｐａｔｈ　ＩＤ）を与えるステップと、各ノードにノードパスＩＤに応じて任意のシードキー（ｓｅｅｄ　ｖａｌｕｅ　ｋｅｙ）を与えるステップと、与えられた任意のシードキーにハッシュ関数を繰り返し適用してキー値を生成するステップと、生成されたキー値を各ノードに順次与えるステップと、を含む。
【選択図】図３



【特許請求の範囲】
【請求項１】
暗号化のためのユーザキー管理方法において、
環状のグループを形成する各ノードにノードパスＩＤを与えるステップと、
前記ノードパスＩＤに応じて前記各ノードに任意のシードキーを与えるステップと、
前記与えられた任意のシードキーに任意の長さの入力値を定められた長さの出力値に圧縮する関数を繰り返し適用してキー値を生成するステップと、
前記生成されたキー値を前記環状のグループを形成する各ノードに順次与えるステップと、
を含むことを特徴とするユーザキー管理方法。
【請求項２】
前記環状のグループ内のＮ個のノードからなる循環区間に対する暗号化キーは、
前記区間内の一番目ノードに与えられた前記シードキーに前記関数をＮ－１回繰り返し適用して生成されたキー値にすることを特徴とする請求項１に記載のユーザキー管理方法。
【請求項３】
前記循環区間は認証されたノードからなる連続区間であることを特徴とする請求項２に記載のユーザキー管理方法。
【請求項４】
前記環状のグループを形成する各ノードの下方に新たな環状のグループを形成するノードを下部構造としてリンクさせることにより、環状のグループの階層構造を形成することを特徴とする請求項１に記載のユーザキー管理方法。
【請求項５】
前記階層構造は１６層であることを特徴とする請求項４に記載のユーザキー管理方法。
【請求項６】
前記各環状のグループを形成している各ノードの個数は同一であることを特徴とする請求項４に記載のユーザキー管理方法。
【請求項７】
前記環状のグループ内のＮ個のノードからなる循環区間は、１つ以上の除外されたノードを含み、前記除外されたノードでは任意の長さの入力値を定められた長さの出力値に圧縮する関数をそれぞれ独立的に適用することを特徴とする請求項１に記載のユーザキー管理方法。
【請求項８】
前記環状のグループを形成するノードはＮ個であり、前記ノードパスＩＤとして０からＮ－１までが与えられることを特徴とする請求項１に記載のユーザキー管理方法。
【請求項９】
前記階層構造において少なくとも１つの除外された子ノードを有するノードは、除外されたノードとしてみなされることを特徴とする請求項４に記載のユーザキー管理方法。
【請求項１０】
前記関数は、ＨＢＥＳ　ＳＨＡ－１であることを特徴とする請求項１に記載のユーザキー管理方法。
【請求項１１】
キー割り当て方法において、
環状のグループを形成する各ノードにノードパスＩＤを割り当てるステップと、
前記環状のグループの第１ノードの複数の第１キーのうちの一つで第１シードを割り当てる第１割り当てステップと、
前記環状のグループの第２ノードで割り当てられた第２シードに任意の長さの入力値を定められた長さの出力値に圧縮する関数を少なくとも一回適用した結果を、前記環状のグループの前記第１ノードの前記複数の第１キーのうちの他の一つに割り当てる第２割り当てステップと、

を含むことを特徴とするキー割り当て方法。
【請求項１２】
前記第１シード及び前記第２シードは、ランダムに生成され、互いに独立していることを特徴とする請求項１１に記載のキー割り当て方法。
【請求項１３】
前記関数は、ＨＢＥＳ　ＳＨＡ－１であることを特徴とする請求項１１に記載のキー割り当て方法。
【請求項１４】
前記環状のグループは、ｔ個のノードを含み、
前記第１ノードは前記環状のグループの第１位置に配列され、前記第２ノードは前記環状のグループの第２位置に配列され、前記第２割り当てステップは、前記第２シードにハッシュ関数を（ｔ－１）回適用するステップを含むことを特徴とする請求項１１に記載のキー割り当て方法。
【請求項１５】
前記環状のグループで前記第１ノードと第２ノードとは、同一の親（Ｐａｒｅｎｔ）ノードを有することを特徴とする請求項１１に記載のキー割り当て方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロードキャスト暗号化方法に関し、詳細にはブロードキャスト暗号化のための効率的なユーザキー管理方法に関する。
【背景技術】
【０００２】
ブロードキャスト暗号化（Ｂｒｏａｄｃａｓｔ　Ｅｎｃｒｙｐｔｉｏｎ：以下、ＢＥと称する）は、全ユーザのうち送信先（即ち、放送センター）が希望するユーザにのみ情報を効率よく伝える方法であって、情報の受け取るユーザの集合が任意的かつ動的に変化する場合に効率よく使用されるべきである。ＢＥで最も重要な性質は、希望しないユーザ（例えば、不法ユーザあるいは期間切れユーザ）の排除または除外である。
【０００３】
図１には、一般のブロードキャスト暗号化によるデータ伝送システムのネットワーク構造が示されている。同図に示すように、コンテンツ生産者１００は、オーディオまたはビデオデータを始めた種々の有効なデータを生産し、生産されたデータをサービス提供者１１０に提供する。サービス提供者１１０はコンテンツ生産者からのデータを種々の有無線通信ネットワークを介して該当のデータに対するコストを支払っている正当ユーザ（例えば、モバイルＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔ　Ｍａｎａｇｅｍｅｎｔ）ネットワーク１４０、スマートホームＤＲＭネットワーク１５０））にブロードキャストする。
【０００４】
つまり、サービス提供者１１０は衛星１２０を介して色々な衛星受信機の備えられたセットトップボックス１４１のようなユーザ装置にデータ伝送が可能になり、移動通信網を介して移動通信端末１４２にも伝送できる。さらに、インターネットネットワーク１３０を介してスマートホームネットワーク１５０の端末１５０、１５１，１５２，１５３，１５４，１５５に伝送できる。
【０００５】
一方、この際に該当データに対する正当なコストを支払っていない不法ユーザ１６０がデータの利用を防ぐためにブロードキャスト暗号化によりデータの暗号化を行う。
【０００６】
かかる暗号化および復号化システムにおける安定性は暗号化キーを管理しているシステムにかかっていると言える。そして暗号化キーシステムにおいて最も重要なのが暗号化キーをどのように生成するか、また、生成された暗号化キーをどのように管理し、更新するかである。

【０００７】
１９９１年ＢＥの概念が提案された以来に数多い変化を経て、今のＢＥは支配されない受信者（ｓｔａｔｅｌｅｓｓ　ｒｅｃｅｉｖｅｒ）を仮定する。この概念はセッション（ｓｅｓｓｉｏｎ）が変わることにより、それぞれのユーザの暗証キーが変えられることなく、また更新されないことを意味する。なお、安定性においては「ｋ－復旧（ｋ－ｒｅｓｉｌｉｅｎｔ）」という用語を使用するが、これは除外されたユーザのうちｋ名が共謀攻撃をしても情報を復旧し切れないことを意味する。大体ｒは除外されたユーザの数を示しているので、「ｒ－復旧（ｒ－ｒｅｓｉｌｉｅｎｔ）」は除外されたユーザ全てが集まって共謀攻撃しても安全であることを意味する。
【０００８】
一方、ＢＥでは伝送量、保存量、計算量を重要視しているが、それぞれの伝送側から伝送すべきヘッダー量、ユーザが保存しなければならない暗証キーの量、およびユーザがセッションキーを獲得するために求められる計算の量を意味する。この中からも伝送量の軽減が最も大きい課題とも言える。伝送量は初期に全ユーザの数であるＮ値に比例したのが、今は主に除外されたユーザの数であるｒに比例し、減少している。伝送量がｒに比例する技術が出現してから伝送量ｒの未満に減少させることがＢＥにおける大きいな課題となっている。
【０００９】
かかるＢＥ問題を基盤にして、今まで発表された結果において「Naor-Naor-Lotspiech」によって発表された「Subset Difference(SD)Method」が優れた結果を挙げている。ＳＤ方法では全ユーザがｎ名である場合、Ｏ（ｌｏｇ$^{3/2}$ｎ）の保存量とＯ（２ｒ－１）の伝送量を要する。
【００１０】
しかしながら、このようなＳＤ方法に基づいても多数のユーザが使用するには効率的な限界が残っているという問題がある。
【００１１】
前述のように、１９９１年BerkovitsがＢＥに関する論文を最初発表した以来、今まで様々なアルゴリズムが提示されていきた。そのうちアルゴリズムについて整理してみると、暗証キー共有（ｓｅｃｒｅｔ　ｓｈａｒｉｎｇ）方法、サブネットカバーフリシステムモデル（Ｓｕｂｓｅｔ　Ｃｏｖｅｒ－Ｆｒｅｅ　Ｍｏｄｅｌ）方法、ツリー構造を用いた方法などが提案されてきた。
【００１２】
最初に、暗証キー共有に基づいたモデルについて概略的に説明する。暗証キー共有モデルは、１９９１年「Ｓ．Ｂｅｒｋｏｖｉｔｓ」により初提案され、2000年「Ｍ．Ｎｏａｒ」と「Ｂ．Ｐｉｎｋａｓ」が「Efficient Trace and Revoke Schemes」という論文でより効率よく改善された。Ｓ．Ｂｅｒｋｏｖｉｔｓの「How to Broadcast a Secret」では、多項式補間（polynomial interpolation）を用いた方法とベクトル基盤暗証キー共有（vector based secret sharing）を用いた方法が提示された。
【００１３】
多項式補間方法によると、センタ（ｃｅｎｔｅｒ；放送センターまたは送信先）から各ユーザに暗証チャネルに点（x_i、y_i）を伝送する。なお、x_iは全て異なる値であり、（x_i、y_i）は各ユーザの暗証キーである。それから、各セッションの正当なユーザｔ名に暗証情報Ｓをブロードキャストするために、ランダム整数ｊと次数ｔ＋ｊ＋１である多項式Ｐを選択する。多項式Ｐはｔ名の正当なユーザ暗証キー（x_i、y_i）と別のユーザの暗証キーでもない任意のｊ個の点（ｘ、ｙ）と（Ｏ，Ｓ）を介する多項式である。そして、センタでは多項式Ｐ上のｔ＋ｊ個の上記点とは異なる点を伝送する。すると、ｔ名の正当ユーザはｔ＋ｊ個以外に１つの点（自分の暗証キー）を知っているので、次数ｔ＋ｊ＋１である多項式Ｐを復旧することができ、暗証情報Ｓも求めることができる。しかし、除外されたユーザは単にｔ＋ｊ個の点のみを知っていることから、絶対多項式Ｐを復旧することができない。

【００１４】
かかる方法は、伝送量がＯ（ｔ＋ｊ＋１）、保存量がＯ（１）、計算量が約ｔ^{3}番の乗算である。さらに、廃棄が容易でかつ共謀を防止することができ、共謀追跡も可能である長所がある。しかし、数多いユーザに対しては非効率的であり、繰り返して使用する場合安全ではないので、実際には使用できない問題がある。
【００１５】
M.NoarとB.Pinkasの「Efficient Trace and Revoke Schemes」については、ラグランジュの補間方式（lagrange’s interpolation formula）を用いた閾値暗証キー共有方式を使用する。Noar－Pinkas方法では、ｒ次多項式をｒ＋１個の多項式上の点を知っていればその復旧が可能であるが、１つ足りないｒ個の点をもっては復旧できないという性質を用いる。即ち、センタは任意のｔ次多項式Ｐを選択し、その上の相異なる点を各ユーザに暗証キーとして提供する。ｒ名のユーザが除外されると、センタは除外されたｒ名の暗証キーと任意に選択されたｔ－ｒ個の点を和して、総ｔ個の点に対する情報をブロードキャストする。その結果、除外されたユーザは自分の秘密情報を加えても依然としてｔ個の点しか知らない一方、除外されないユーザはｔ＋１個の点を知っていることから、多項式Ｐの復旧が可能になる。この多項式を用いてセッションキーＰ（０）値を求めることができる。
【００１６】
かかる方法も廃棄し易く、かつ共謀も防止できるので、共謀追跡も可能である。特に、新たなユーザを追加（ａｄｄ）できるという大きな長所があり、伝送量がＯ（ｔ）で保存量はＯ（１）であるという効率性を有する。しかし、このような方法によると、最初に定められたｔより多いユーザを除外することはできない問題がある。さらに、伝送する点の数や多項式を算出するために求められる計算量がｔに依存することになり、非効率的になる。また、ｔが大きくなるほど算出時間が増大してしまい、多数のユーザを含んでいる場合には不都合である。
【００１７】
第２に、サブセットカバーフリシステムモデルは、全てのユーザの集合をＳであるとすると、Ｓのサブセットを元素としてする集合でサブセットカバーフリシステムという概念を定義する。かかるシステムを探すことができればそのシステムを用いてＢＥを行うことができる。しかし、保存量と伝送量がＯ（ｒ ｌｏｇ ｎ）程度になり効率ではないという短所がある。さらに、１－ｒｅｓｉｌｉｅｎｔ モデルを拡張してｋ－ｒｅｓｉｌｉｅｎｔモデルにする方法も紹介された。効率的な１－ｒｅｓｉｌｉｅｎｔ方法は考案し易いことから、そのような拡張が意味のあるようにみえるが、今まで提示された方法としては拡張する過程でその効率性が落ちてしまう問題がある。
【００１８】
第３に、最近にはツリー構造を用いる方法が注目を浴びている。１９９８年にC.K.Wong, M.Gouda, G.S.LamからLTH(Logical-tree-hierarchy)方法が提案されたが、一回のセッションから数多いユーザを除外するには無理が伴う。さらに、ユーザの暗証キーはセッションの変化により共に変化するので、支配されない受信先（ｓｔａｔｅｌｅｓｓ ｒｅｃｅｉｖｅｒ）を仮定する現代的なＢＥとは距離感がある。その後、２００１年D.Naor, M.Naou, J.Lotspiechが 「Complete Subset(CS) Cover Scheme」と「Subset Difference(SD) Scheme」を提案した。２つの方法共にユーザの数はｎ名、除外されたユーザの数はｒであると仮定し、センタは高さのｌｏｇ ｎである２進ツリー（ｂｉｎａｒｙ ｔｒｅｅ）をつくり、全てのノードにはそれに対応する暗証キーを割り当てる。そして、葉ノード（ｌｅａｆ ｎｏｄｅ）にユーザを一人ずつ割り当てる。
【００１９】
最初に、ＣＳ Ｃｏｖｅｒ方法について説明すると、各ユーザはルーツノード（ｒｏｏｔ ｎｏｄｅ）から自分の葉ノードまでの経路に位置する全てのノードの暗証キーをセンタから受けて保存する。ここで、サブツリーのうち除外されたユーザを１名も含まない完全なサブツリーを「ｃｏｍｐｌｅｔｅ Ｓｕｂｔｒｅｅ（ＣＳ）」というが、このような

ＣＳを適当に集めると、除外されないユーザのみを全て含ませることができる。なお、使用されたＣＳのルーツノードに当たる暗証キーでセッションキーを暗号化し伝送すると、正当なユーザはセッションキーを復旧することはできるものの、除外されたユーザは上に使用されたいずれのＣＳにも含まれないことから、セッションキーの復旧をすることができない。

【００２０】

図２は従来のツリー構造でキーの割り当てを行うブロードキャスト暗号化の概念を示す図面である。同図に示すように、ブロードキャスト暗号化方式を介してデータの提供された各ユーザ２２０はそれぞれ自分の固有のキー値（３２ないし４７）を有すると同時に、ツリー構造上で自分と連結した各ノードのキー値を有することになる。

【００２１】

例えば、３４番ユーザは自分の３４番キー値と共に１７番ノード２０９のキー値、８番ノード２０４のキー値、４番ノード２０２のキー値、２番ノード２０１のキー値を有することとなる。この際に、前記３４番ユーザが有する１７番目ノード２０９のキー値は３５番ユーザも共に共有される。同様に、前記３４番ユーザが有する８番ノード２０４のキー値は３２，３３，３５番ユーザも共に共有する。

【００２２】

一方、３２番ないし４７番ユーザが全て正当なユーザである場合、好ましくは伝送しようとするデータのヘッダ部分に２番ノード２０１キー値を含んで全てのユーザへ同一に伝送することによってセキュリティの保障されたデータ伝送が行われる。

【００２３】

しかし、もし３６番ユーザ２２１のキーを有するユーザが正当なユーザではない不法ユーザ（ｒｅｖｏｋｅｄ　ｕｓｅｒ）である場合、前記３６番ユーザ２２１と関連したノードのキー値を有する他のユーザが共有していることから、該当のキー値を更新してくれる過程が必要とされる。即ち、１８番ノード２１０、９番ノード２０５、４番ノード２０２、および２番ノード２０１のキー値を更新しなければならない。なお、前記キー値を更新するためには下位ノードから上位ノードの順で行われる。

【００２４】

まず、前記１８番ノード２１０のキー値は３７番ユーザが共有しているので、サーバから１８番ノード２１０の更新されたキー値を３７番ユーザのキー値で暗号化し３７番ユーザに伝送する。それから、９番ノード２０５のキー値は３７番ユーザと共に、１９番ノード２１１下にある３８番ユーザおよび３９番ユーザが共に共有しているので、９番ノード２０５の更新されたキー値を３７番ユーザには予め更新された１８ノード２１０のキー値で暗号化して伝送し、３８番および３９番ユーザには１９番ノード２１１のキー値で暗号化して伝送する。

【００２５】

同様の方法で、４番ノード２０２のキー値は８番ノード２０４の下にある３２，３３，３４，３５番ユーザと共に、９番ノード２０５の下にある３７，３８，３９番ユーザが共に共有しているので、４番ノード２０２の更新されたキー値を３２ないし３５番ユーザには８番ノード２０４のキー値で暗号化して伝送し、３７，３８，３９番ユーザには予め更新された９番ノード２０５のキー値で暗号化して伝送する。

【００２６】

最後に、２番ノード２０１のキー値は４番ノード２０２の下にある３２ないし３９番ユーザのうち３６番ユーザ２２１を除いたユーザが共有し、５番ノード２０３の下にある４０ないし４７番ユーザが共に共有しているので、２番ノード２０１の更新されたキー値を３２、３３，３４，３５，３７，３８，３９番ユーザには予め更新された４番ノード２０２のキー値で暗号化して伝送し、４０ないし４７番ユーザには５番ノード２０３のキー値で暗号化して伝送する。かかるキー更新過程を介して不法（あるいは廃止された）ユーザの接近を遮断することが可能となる。

【００２７】

前述した方法（つまり、ＣＳモデル）における伝送量は全て除外されないユーザのみを含ませるＣＳの個数であるＯ（ｒ　ｌｏｇ（ｎ／ｒ））であり、保存オーバーヘッドはＯ（ｌｏｇ　ｎ）である。

【００２８】

一方、ＳＤ（Ｓｕｂｓｅｔ　ｄｉｆｆｅｒｅｎｃｅ）モデルは、前述のＣＳモデルの変形であって、Ｏ（ｌｏｇ^{2}　ｎ）の保存量とＯ（２ｒ－１）の伝送量を要求し伝送力の画期的な改善を図った。ＳＤモデルでは、１つのノードｖをルーツとするサブツリーから該当サーブツリーに含まれた他の１つのノードｗをルーツとするサブツリーを引いたサブツリーについて考案する。このサブツリーの下の葉ノードは正当なユーザであり、ｗをルーツとしてするサブツリーの下の葉ノードは除外されたユーザである。かかる方法は適当な数の正当ユーザとの間に除外されたユーザが存在する場合、ＣＳモデルが必ず２つ以上のサブセットを必要とするのとは相違に、１つのサブセットでカバーすることができる。ＳＤ方法は、ノードｖに割り当てられたキーのハッシュ（ｈａｓｈ）値から始まってノードｗまでのハッシュ値を求め、その値に対応する値をセッションキーとしてする。各ユーザはルーツノードから自分の葉ノードまでのパス上の各ノードに対する兄弟ノード（ｓｉｂｌｉｎｇ　ｎｏｄｅ）に対するハッシュ値を暗証キーとして有している。従って、ハッシュ関数の一方向性により正当なユーザのみがセッションキーの復旧を行うことができる。なお、ＳＤモデルの伝送量はＯ（２ｒ－１）、保存量はＯ（ｌｏｇ^{2}ｎ）であり、計算量は最大Ｏ（ｌｏｇ　ｎ）のハッシュにしか及ばない。

【００２９】

その後、２００２年にはＳＤモデルの改善されたＬＳＤモデルが提案された。ＬＳＤモデルでは各サブツリーにレイヤーを用いて保存量をＯ（ｌｏｇ^{3}／^{2}ｎ）に減らした変わりに伝送量がＳＤモデルの２倍となった。

【００３０】

前述したＢＥモデルのうち優れた効率をみせたのがＬＳＤやＳＤなどのツリー構造を使用したモデルであった。しかし、前記ツリー構造を用いた方法は、ブロードキャストに求められるサブセットの数がユーザの位置に大きく依存することから、それ以上の改善は期待し難い。さらに、ツリー構造の場合、メンテナンスにも相当なコストがかかってしまう短所があるので、前述したツリー構造ではないより効率のよいＢＥ技術が求められている実情がある。

【先行技術文献】

【特許文献】

【００３１】

【特許文献１】特開平１５－２７３８５８号公報

【特許文献２】特開平０７－００５８０８号公報

【特許文献３】特開平１４－１２４９５２号公報

【発明の概要】

【発明が解決しようとする課題】

【００３２】

本発明は前述した問題点を解決するために案出されたもので、本発明の目的は、線形構造を用いて各ノード別に順次に一方向キーチェーンを形成してキー値を分配するブロードキャスト暗号化のためのユーザキー管理方法を提供することにある。

【００３３】

さらに、本発明の目的は、線形構造を用いて直線上のノードから毎ｃ番目ノードを選択し特別ノードとして設定し、特別ノードキーから開始する特別ノードチェーンを生成するブロードキャスト暗号化のためのユーザキー管理方法を提供することにある。

【００３４】

さらに、本発明の目的は一人の除外されたユーザを含んでいる区間を追加して伝送区間を設定し、伝送量を減らすことのできるブロードキャスト暗号化のためのユーザキー管理方法を提供することにある。

【課題を解決するための手段】
【００３５】
前述の目的を達成するための本発明にかかるキー管理方法は、順次配列された各ノードにノードパスＩＤ（Ｎｏｄｅ　Ｐａｔｈ　ＩＤ）を与えるステップと、前記各ノードに前記ノードパスＩＤに応じて任意のシードキー（ｓｅｅｄ　ｖａｌｕｅ　ｋｅｙ）を与えるステップと、前記与えられた任意のシードキーにハッシュ関数を繰り返し適用してキー値を生成するステップと、
前記生成されたキー値を前記各ノードに順次与えるステップと、を含む。
【００３６】
好ましくは、前記順次配列されたノードのうちＮ個のノードからなる区間に対する暗号化キーは、前記区間内の一番目ノードに与えられた前記シードキーに前記ハッシュ関数をＮ－１回繰り返し適用して生成されたキー値にすることを特徴とする。
【００３７】
さらに、前記区間は認証されたノードからなった連続区間であることを特徴とする。
また、前記区間は１つ以上の除外されたノードを含み、前記除外されたノードではそれぞれ独立的にハッシュ関数を適用することを特徴とする。
【００３８】
一方、本発明に係るキー管理方法は、順次配列された各ノードに任意のシードキーを与えるステップと、前記与えられた任意のシードキーに第１ハッシュ関数を繰り返し適用してキー値を生成するステップと、前記生成されたキー値を前記各ノードに順次与えるステップと、前記順次配列されたノードのうち一定の間隔に応じて特別ノードを設定するステップと、前記各特別ノードには任意の特別シードキーを与えるステップと、前記与えられた任意の特別シードキーに第２ハッシュ関数を繰り返し適用してキー値を生成するステップと、前記生成されたキー値を前記各特別ノードに順次与えるステップと、を含む。
【００３９】
好ましくは、前記特別ノードのうち第１特別ノードにＫという特別ノードキーが与えられると、前記第１特別ノードから前記一定の間隔だけ離れた第２特別ノードには前記Ｋに前記第２ハッシュ関数を適用したキー値が与えられることを特徴とする。
【００４０】
また、前記順次配列されたノードのうちＮ個のノードからなる区間に対する暗号化キーは、前記区間内の一番目ノードに与えられた前記シードキーに前記ハッシュ関数をＮ－１回繰り返し適用して生成されたキー値にすることを特徴とする。
【００４１】
また、前記区間は認証されたノードからなった連続区間であることを特徴とする。
【００４２】
また、前記区間は１つ以上の除外されたノードを含み、前記除外されたノードではそれぞれ独立的に新たなハッシュ関数を適用することを特徴とする。
【００４３】
一方、本発明に係るキー管理方法は、環状のグループを形成する各ノードにノードパスＩＤを与えるステップと、前記各ノードに前記ノードパスＩＤに応じて任意のシードキーを与えるステップと、前記与えられた任意のシードキーにハッシュ関数を繰り返し適用してキー値を生成するステップと、前記生成されたキー値を前記環状のグループを形成する各ノードに順次与えるステップと、を含む。
【００４４】
好ましくは、前記環状のグループ内のＮ個のノードからなる循環区間に対する暗号化キーは、前記区間内の一番目ノードに与えられた前記シードキーに前記ハッシュ関数をＮ－１回繰り返し適用して生成されたキー値にすることを特徴とする。
【００４５】
また、前記循環区間は認証されたノードからなった連続区間であることを特徴とする。
【００４６】

また、前記環状のグループを形成する各ノードの下方に新たな環状のグループを形成するノードを下部構造としてリンクさせることにより、環状のグループの階層構造を形成することを特徴とする。

【００４７】

前記階層構造は１６層であることを特徴とし、前記各環状のグループを形成している各ノードの個数は同一であることを特徴とする。

【００４８】

さらに、前記環状のグループ内のＮ個のノードからなる循環区間は、１つ以上の除外されたノードを含み、前記除外されたノードではそれぞれ独立的なハッシュ関数を適用することを特徴とする。

【００４９】

また、前記環状のグループを形成するノードはＮ個であり、前記ノードパスＩＤとして０からＮ－１までが与えられることを特徴とする。

【００５０】

さらに、前記階層構造において少なくとも１つの除外された子ノードを有するノードは、除外されたノードとしてみなされることを特徴とする。

【００５１】

一方、本発明に係るキー管理方法は、環状のグループを形成する各ノードに任意のシードキーを与えるステップと、前記与えられた任意のシードキーに第１ハッシュ関数を繰り返し適用してキー値を生成するステップと、前記生成されたキー値を前記環状のグループを形成する各ノードに順次与えるステップと、前記環状のグループを形成するノードのうち一定の間隔に応じて特別ノードを設定するステップと、前記各特別ノードには任意の特別シードキーを与えるステップと、前記与えられた任意の特別シードキーに第２ハッシュ関数を繰り返し適用してキー値を生成するステップと、前記生成されたキー値を前記各特別ノードに順次与えるステップと、を含む。

【００５２】

好ましくは、前記特別ノードのうち第１特別ノードにＫという特別ノードキーが与えられると、前記第１特別ノードから前記一定の間隔だけ離れた第２特別ノードには前記Ｋに前記第２ハッシュ関数を適用したキー値が与えられることを特徴とする。

【００５３】

また、前記環状のグループ内のＮ個のノードからなる循環区間に対する暗号化キーは、前記循環区間内の一番目ノードに与えられた前記シードキーに前記ハッシュ関数をＮ－１回繰り返し適用して生成されたキー値にすることを特徴とする。

【００５４】

また、前記循環区間は認証されたノードからなった連続区間であることを特徴とする。

【００５５】

また、前記循環区間は１つ以上の除外されたノードを含み、前記除外されたノードではそれぞれ独立的に新たなハッシュ関数を適用することを特徴とする。

【発明の効果】

【００５６】

本発明によると、ブロードキャスト暗号化にて最も重要な伝送量をｒ未満に減らすことができる。さらに、本発明の実施形態では今まで優先的な方法として知られたＳＤと比較して伝送量を大いに減らし得る長所がある。

【００５７】

さらに、本発明によると、多数のユーザが共謀しても新たなキーを作り出すことができず、不法デコーダが作られた場合に共謀したユーザキーがそのまま使用されるので追跡できる長所がある。最後に、シーケンスの後ろ部分に、希望するだけのユーザを自在に追加できる。

【図面の簡単な説明】

【００５８】

【図１】一般のブロードキャスト暗号化によるデータ伝送システムのネットワーク構造を示す図面である。
【図２】従来のツリー構造であって、キーを割り当てるブロードキャスト暗号化の概念を示す図面である。
【図３】本発明の実施形態に係る線形構造の各ノードに一方向キーチェーンをマッピングしてキー値を与える手続きを示すフローチャートである。
【図４】本発明の実施形態に係る線形構造の各ノードに任意のシードキーを与える方法を示す図面である。
【図５】本発明の実施形態に係る線形構造の各ノードに一方向キーチェーンをマッピングする方法を示す図面である。
【図６】本発明の実施形態に係る線形構造の各ノードにキー値を対応させる方法を示す図面である。
【図７】本発明の実施形態に係る線形構造の各ノードにキー値が対応された結果を示す図面である。
【図８】本発明の実施形態に係る不法ユーザとの間の区間へのセッションキー伝達手続きを示すフローチャートである。
【図９】本発明の実施形態に係る線形構造での区間の定義を示す図面である。
【図１０】本発明の実施形態に係る線形構造の区間であって、セッションキーを伝達する方法を示す図面である。
【図１１】本発明の実施形態に係る各ノードのユーザが受信されたセッションキーによりデータを復号化する手続きを示すフローチャートである。
【図１２】本発明の変形された第１の実施形態に係る線形構造での特別ノードの定義を示す図面である。
【図１３】本発明の変形された第１の実施形態に係る線形構造での各ノードにキー値を対応させる方法を示す図面である。
【図１４】本発明の変形された第１の実施形態に係るセッションキー伝送のために区間を分ける方法を示す図面である。
【図１５】本発明の変形された第１の実施形態に係る多数の区間に分けられた場合にセッションキーを伝送する方法を示す図面である。
【図１６】本発明の変形された第２の実施形態に係る区間設定方法を示す図面である。
【図１７】本発明の変形された第２の実施形態に係る線形構造での各ノードにキー値を対応させる方法を示す図面である。
【図１８】本発明の変形された第４の実施形態に係る環状構造の各ノードにキー値が対応された結果を示す図面である。
【図１９】本発明の一実施形態に係る環状構造の各ノードグループの階層構造を示す図面である。
【発明を実施するための形態】
【００５９】
以下、添付の図面に基づいて本発明の好適な実施形態を詳述する。
＜基本実施形態＞
【００６０】
図３は、本発明の実施形態に係る線形構造の各ノードに一方向キーチェーンをマッピングしてキー値を与える手続きを示すフローチャートである。同図に示すように、まず、それぞれのノードにノードパスＩＤを与える（Ｓ３０１）。ここで、ノードパスＩＤは各ノードに該当するユーザを区分するためのＩＤである。
【００６１】
それから、線形構造上の各ノード別にノードパスＩＤに応じて任意のシードキー（ｓｅｅｄ　ｖａｌｕｅ　ｋｅｙ）を与える（Ｓ３０２）。本発明を実施するに当たり、任意のシードキーはそれぞれ独立的に、かつランダムに決定され得る。
【００６２】

それから、各ノード別に与えられた任意のシードキーを一方向ハッシュ関数に代入した結果であるキー値を生成する。さらに、生成されたキー値を一方向ハッシュ関数に繰り返して代入することでキー値が連続的に生成され、各任意のシードキーに応じて各所定のキーチェーンを生成する（Ｓ３０３）。

【００６３】

ここで、一方向ハッシュ関数とは、任意の長さの入力値を定められた長さの出力値として圧縮する関数であって、次のような性質を持つ。一方向ハッシュ関数上では、与えられた出力値について入力値を求めることが計算上できず、与えられた入力値を出す更なる入力値を探し出すことは計算上できない。また、一方向ハッシュ関数上では同一出力値を出す任意の相異なる２つの入力値を探すことも計算上できない。

【００６４】

前述のような性質を満たすハッシュ関数は、データの完全性、認証、否認防止などで応用される重要な関数の１つであって、本発明を実施するための一方向ハッシュ関数は「ＨＢＥＳ　ＳＨＡ－１」になり得る。

【００６５】

Ｓ３０３における各シードキー別に生成されたキー値を各シードキーの与えられたノードの次ノードから順次与えられる（Ｓ３０４，３０５）。本発明を実施するにあたって、キー値が与えられる方法は各ノードにおいて一定性を有するべきである。

【００６６】

以下、図４ないし図６に基づいて前述したキー値が各ノードに与えられる手続きについて詳説する。

【００６７】

図４には本発明の実施形態に係る線形構造の各ノードに任意のシードキーを与える方法が図面されている。同図に示すように、各ノード別任意のシードキーは直線状の各ノードに前の方から順次マッピングされることができる。

【００６８】

例えば、同一空間にＮ個のノードが配列されたと仮定し、各ノードにはランダムに選択されたシードキー値であるK_1，K_2，...K_N値が１つずつ対応される。即ち、第１ノード４０１にはK_1値、第２ノード４０２にはK_2値、第３ノード４０３にはK_3値、第４ノード４０４にはK_4値...、第Ｎ－１ノード４０５にはK_{N-1}値、第Ｎノード４０６にはK_N値のランダムに選択されたシード値が対応される。

【００６９】

この時、前述した各シードキーから一方向ハッシュ関数を用いて一方向キーチェーンが生成されるようになる。一方向キーチェーンを生成する方法は次の通りである。

【００７０】

もし、ｈが$\{0,1\}^{128} \rightarrow \{0,1\}^{128}$である一方向ハッシュ関数であると、Ｋからの長さｃである一方向キーチェーンは{Ｋ，ｈ（Ｋ）、ｈ（ｈ（Ｋ））＝$h^{(2)}$（Ｋ）、...$h^{(c-1)}$（Ｋ）}になる。前記生成された一方向キーチェーン値は前の方から順次に直線状の各ノードへ対応される。

【００７１】

図５は本発明の実施形態に係る線形構造の各ノードに一方向キーチェーンをマッピングする方法を示す図面である。同図に示すように、一方向ハッシュ関数であるｈを用いて各ノードで始まる長さｃである一方向キーチェーンを生成してマッピングする。ここで、前記ｃはチェーンのサイズを意味する。

【００７２】

即ち、第ｉノード５０１にはシードキー値であるK_1値がマッピングされ、第ｉ＋１ノード５０２にはｈ（K_i）値がマッピングされ、第ｉ＋２ノード５０３にはｈ（ｈ（K_i））値がマッピングされ、...、第ｉ＋ｃ-１ノード５０４には$h^{(c-1)}$（K_i）値がマッピングされる。

【００７３】

一方、本発明の実施形態において、一方向キーチェーンの長さを決定する値としてｃ値を予め設定し、前記ｃ値に応じて各ユーザが保存しなければならないキーの数が決定されるのである。従って、各ノードに与えられた全てのシードキーから長さｃである一方向キーチェーンを生成することができ、生成された一方向キーチェーン値は各ノードに与えられる。

【００７４】

その結果、それぞれのノードには全てｃ個のキー値が与えられることになる。但し、直線の開始部分と終了部分の一部ノードにはより少ない数のキーが割り当てられる。即ち、各ユーザの保存量はＯ（ｃ）になる。

【００７５】

図６には本発明の実施形態に係る線形構造の各ノードにキー値を対応させる方法が図示されている。同図に示すように、第ｉノード６０１には自分のシードキーであるK_i値が与えられ、第ｉ＋１ノード６０２にはK_iを一方向ハッシュ関数演算値であるｈ（K_i）と予め与えられた自分のキー値であるK_{i+1}が与えられる。さらに、第ｉ＋２ノード６０３には、第ｉ＋１ノード６０２に与えられたキー値を一方向関数演算した値と予め与えられた自分のキー値とが与えられる。

【００７６】

即ち、K_iを２回一方向ハッシュ関数演算した値であるｈ（ｈ（K_i））と、K_{i+1}を一方向ハッシュ関数演算した値であるｈ（K_{i+1}）と、自分のシードキー値であるK_{i+2}が与えられる。同じ方法に基づいて、ｃ番目ノードである第ｉ＋ｃ－１ノード６０５は$h^{(c-1)}(K_i)$、$h^{(c-2)}(K_{i+1})$、$h^{(c-3)}(K_{i+2})$、...K_{i+c-1}が与えられる。

【００７７】

従って、各ノード別に対応されるユーザは各ユーザの位置に応じて１個からｃ個までのキーがユーザの暗証キーとして与えられるようになる。

【００７８】

なお、$K_{i,i}=K_i$とし、ｉ≦ｊにおいて$K_{i,j}=h^{(j-i)}(K_{i,j})$と定義すると、ユーザ$u_i$が保存しているキーセットは下記数式の通りである。

【００７９】

【数１】

$$U_i=\{K_{k,j}\mid 0\le i-k\le c, i\ge 1, k\ge 1\}$$

【００８０】

また、上記数１に基づいて、各ノードに割り当てられるキー値は図７に示す表の通りである。図７は本発明の実施形態に係る線形構造の各ノードにキー値が対応された結果である。

【００８１】

同図を参照すると、ユーザu_cのキー値７０１は、図示されたようにｃ個のキー値が割り当てられていることが分かる。それと共に、本発明では全体のユーザを１つ以上の小さい部分集合として分割し、前記分割された各部分集合にセッションキーを１つのイメージを用いて伝える方式が用いられる。

【００８２】

図８には本発明の実施形態に係る不法ユーザ間の区間へのセッションキー伝達手続きが示されたフローチャートである。同図を参照すると、最初に、二人の除外されたユーザ（ｒｅｖｏｋｅｄ　ｕｓｅｒ）との間に位置した正当なユーザの連続された配列を区間として定義し、セッションキーを伝達するために除外されたユーザ間における区間を設定する（Ｓ８０１）。それから、前記設定された各区間を部分集合にしてセッションキーを伝達する（Ｓ８０２）。

【００８３】

この時、除外されたユーザが連続的に位置する場合を除けば、二人の除外されたユーザとの間に１つの区間が作られる。よって、最大ｒ＋１個の区間を用いてセッションキーが伝えられることになる。しかし、本発明の実施形態により、１つの区間当たり最大の長さがｃと制限された場合に、区間の長さがｃより大きい区間についてはより多い伝送量が求められる。

【００８４】

正当なユーザの連続した配列区間を設定する方法について例を挙げて説明すると、まず、U_1ないしU_{10}までのユーザがいて、彼らのうちU_5が除外されたユーザであり、１つの区間の最大長さを５に制限する場合に、U_1ないしU_4までの１つの区間と、U_6ないしU_{10}までの１つの区間が設定される。

【００８５】

さらに、U_1ないしU_{10}までのユーザがいて、彼らのうちU_1およびU_{10}が除外されたユーザであり、１つの区間の最大長さを５に制限する場合に、U_2ないしU_6までの１つの区間と、U_7ないしU_9までの１つの区間が設定される。

【００８６】

図９は、本発明の実施形態に係る線形構造における区間の定義を示した図面である。同図を参照すると、二人の除外されたユーザ（ｒｅｖｏｋｅｄ　ｕｓｅｒ）９０１、９０３との間に位置した連続的に印加されたユーザ（ｐｒｉｖｉｌｅｇｅｄ　ｕｓｅｒ）の集まりを区間９０２として定義する。

【００８７】

一方、前述した区間を設定してから、U_iに当たるノードキーK_iから開始される一方向キーチェーンを確認し（Ｓ８０３）、$h^{(s)}(K_i)$の値をキーとして使用してセッションキー（ＳＫ）を暗号化し送信する（Ｓ８０４）。結局、前記暗号化されたメッセージが伝送されるのである（Ｓ８０５）。

【００８８】

より詳細に説明すると、区間$\{u_i, u_{i+1}, u_{i+2}, \ldots u_{i+S}\}$について（但し、ｓはｃより小さい値である場合）セッションキー（ＳＫ）を伝達するために、センターはu_iに該当するノードキーK_iから開始する一方向キーチェーンを用いる。前記一方向キーチェーンの値からu_{i+S}に対応するキー値である$h^{(s)}(K_i)$の値をキーとして用いて、前記セッションキーを暗号化し送信する。即ち、Ｅ（Ｋ，Ｍ）がＫをキーとする暗証キー暗号アルゴリズムであるとき、$E(h^{(s)}(K_i), SK)$のメッセージを全ユーザに伝送する。

【００８９】

一方、前述したように予め与えられたキー値により前記伝送されたメッセージを復号化できるユーザはキー$h^{(s)}(K_i)$を求めることのできるユーザだけである。従って、区間$\{u_i, u_{i+1}, u_{i+2}, \ldots u_{i+S}\}$に含まれたユーザのみが該当キーを求めることができる。

【００９０】

即ち、前記区間に含まれたユーザはK_iから開始する一方向キーチェーンのうち１つの値を知っていて、前記値が$h^{(s)}(K_i)$より左側に位置しているので、一方向関数ｈを自分の値に適用することで$h^{(s)}(K_i)$が求めるのである。

【００９１】

一方、前記区間に含まれていないユーザのうち区間より左側に位置しているユーザはK_iに関した値を求めることができないので、$h^{(s)}(K_i)$も求められない。さらに、区間の右側に位置しているユーザは、たとえ一方向キーチェーンの一部値を求め得るものの、一方向関数の一方向の性質のことで一方向キーチェーンの左側値は求められない。

【００９２】

これにより、前記該当の区間に含まれていない、いずれのユーザが共謀をするとしても$h^{(s)}(K_i)$を求めることは不可能で、これによりセッションキーも復旧できない。

【００９３】

図１０は本発明の実施形態に係る線形構造の区間であって、セッションキーを伝達する方法が図示されている。同図を参照すると、前述したような本発明の実施形態により１つの区間に含まれたユーザにセッションキー（ＳＫ）を同時に伝えることができる。

【００９４】

即ち、除外されたユーザが第ｉノード１００１と第ｉ＋ｔ＋ｊノード１００５に位置し、前記二人の除外されたユーザの間にｔ＋１名の印加されたユーザ１００２、１００３、１００４があると仮定すれば、前記印加されたユーザのために１つの暗証キーを伝送することができる。つまり、Ｅ（Ｋ、ｍ）がＫをキーとしてする暗証キー暗号方式であるとすれば、前記ユーザu_i、...u_{i+t}のためのセッションキーのヘッダーは次の数式２のように表われる。

【００９５】

【数２】

$$\text{ヘッダ} = E\left(h^{(t)}(K_i), SK\right)$$

【００９６】

図１１は、本発明の実施形態に係る各ノードのユーザが受信されたセッションキーによりデータ復号化の手続きを示すフローチャートである。同図に示すように、前述した方法に基づいて伝送されたキー値により印加されたユーザのみが受信データを復号することができる。即ち、暗号化された前記ヘッダーの含まれたメッセージを受信（Ｓ１１０１）した各ユーザは該当区間内のユーザである場合（Ｓ１１０２）、自分の有しているキー値で前記$h^{(s)}(K_i)$を演算し復号化する（Ｓ１１０３）。一方、該当区間内のユーザでない場合は前記$h^{(s)}(K_i)$の演算ができないことから、受信データの復号化も行うことができない（Ｓ１１０４）。

【００９７】

詳細には、第ｉノード以前のユーザ１００２はK_iの値が分からないのでキー値を求めることができず、第ｉ+ｔ以来のユーザは、たとえK_iの一方向キーチェーンの後ろ部分は知っているものの、一方向ハッシュ関数の一方向性質のことで$h^{(s)}(K_i)$を求めることはできない。

【００９８】

一方、前記区間に含まれた正当な全ユーザは自分の有しているキー値のうちK_iから作られた値にｈを繰り返して適用することで、$h^{(s)}(K_i)$値を求めることができる。

【００９９】

なお、前述した本発明の実施形態において全てのＮ名のユーザからｒ名の除外されたユーザが含まれた場合の伝送量を算出すると次のとおりである。

【０１００】

まず、各ユーザが保存すべきなのが最大にｃ個のキー値である。そのとき伝送量は最悪の場合にｒ+（Ｎ－２ｒ）/ｃ個であって、これは全て除外されたユーザが直線の一方に集まり、残り部分は正当なユーザのみが集まっている場合である。

【０１０１】

さらに、除外されたユーザが２以上で連続に表れる場合は伝送量が減少するので、除外されたユーザと正当なユーザが交番に位置する場合について考える。このときに、Ｎ／ｃが追加に必要な理由は、１回の伝送でキー伝達可能な区間の最大長さをｃとして設定したからである。

【０１０２】

また、ユーザの計算量は、最大にｃ番の一方向関数計算と暗証キー暗号アルゴリズム１回であって、これをＮ＝１，０００，０００、ｒ＝５０，０００である状況で算出してみると下記の結果値が獲得される。

【０１０３】

【表１】

ｃ（保存量）	伝送量（worst case）	ｒａｔｉｏ
５０	50,000＋18,000	１．３６ｒ
１００	50,000＋9,000	１．１８ｒ
２００（約３Ｋ）	50,000＋4,500	１．０９ｒ

【０１０４】
以下、前述した本発明の実施形態の変形例について説明する。最初に、変形された第１の実施形態は、前述した実施形態で区間の長さをｃとして設定することにより伝送量がｒより大になることを補完するため、長い区間について１回の伝送のみでキー値を伝送する方法である。
【０１０５】
更に、変形された第２の実施形態は伝送量をｒより減少させるために除外されたユーザの位置から新たな一方向関数を適用する方法である。それと共に、変形された第３の実施形態は前記変形された第１の実施形態および変形された第２の実施形態を組み合わせた方法である。
【０１０６】
＜変形された第１の実施形態＞
前述の実施形態において伝送量がｒより大になる理由は、区間の長さをｃに限定したからである。従って、伝送量がｒに近づくためには前述した区間限定に応じて求められる伝送量を減らさなければならない。従って、前述した基本概念の拡張により、長い区間について１回の伝送でキーを伝送することのできる拡張された実施形態を提案する。
【０１０７】
本発明の変形された第１の実施形態は、直線上のノードのうち一定間隔（例えば、毎ｃ番目ノード）に応じて特別ノードを設定する。
【０１０８】
前記特別ノード毎に既存のシードキーとは独立的な特別シードキーを再度ランダムに選択して対応させ、前記特別ノードキーから開始する特別ノードチェーンを生成する。
【０１０９】
図１２は本発明の変形された第１の実施形態に係る線形構造における特別ノードが定義されている。同図を参照すると、ｃ番目ノード１２０４、１２０５毎に特別ノード１２０１，１２０２，１２０３を設定する。前記設定されたｃ番目ノード毎に設定された特別ノード１２０１，１２０２，１２０３にそれぞれ特別シードキーを与え、前記キーから長さのｃ×c_2である一方向チェーンが構成される。
【０１１０】
より詳細に説明すると、各特別ノード１２０１，１２０２，１２０３毎に既存のシードキーとは独立的な特別シードキーを再度ランダムに選択して対応させ、新たな一方向ハッシュ関数を用いて各特別シードキー別に、前記特別シードキーから始まる特別ノードチェーンを形成する。
【０１１１】
この際、c_2が新たな定数であると、前記特別ノードチェーンは前述したようにｃ×c_2の長さを有する。
【０１１２】
以下、図１３に基づいて特別ノードに特別ノードチェーンを対応させる方法について説明する。
【０１１３】
図１３には本発明の変形された第１の実施形態に係る線形構造における各ノードにキー値を対応させる方法が図示されている。変形された第１実施形態においてチェーンを形成する方法は、基本的に前述した基本実施形態と同様な方法に基づく。しかし、次の区間{

u_i、u_{i+1}、u_{i+2}、...u_{i+S}}が特別ノードから始まる長さがｃを超える区間であるとするとき、前記区間に対するキー伝送はu_iから開始される特別ノードチェーンによりなされる。この時、ＳＫを暗号化する方式は前述の基本実施形態から同様である。即ち、u_iから開始されるチェーンのu_{i+s}に対応する値を用いてＳＫを暗号化し伝送する。

【０１１４】

図１３に基づくと、第ｃノードである第１特別ノード１３０１にＫという特別ノードキーが割り当てられると、長さｃが超えた第２ｃノードである第２特別ノード１３０２には前記Ｋを新たな一方向関数$h_2$１３０４に一方向関数演算したh_2（Ｋ）の特別ノードキー１３０５が割り当てられる。同様に、第３ｃノードである第３特別ノード１３０３には前記Ｋを新たな一方向関数$h_2$１３０４に２回一方向関数演算（つまり、$h_2^{(2)}$１３０６）した$h_2^{(2)}$（Ｋ）が与えられる。

【０１１５】

従って、第ｃ＋１ノードでは第ｃノードの特別シードキーＫをｈにより一方向関数演算したｈ（Ｋ）が与えられ、第ｃ＋２ノードでは第ｃノードの特別シードキーＫをｈにより２回一方向関数演算した$h^{(2)}$（Ｋ）が与えられる。同様に、第２ｃ＋１ノードでは第２ｃノードに与えられたh_2（Ｋ）をｈにより一方向関数演算したｈ（h_2（Ｋ））が与えられ、第３ｃ＋１ノードでは第３ｃノードに与えられた$h_2^{(2)}$（Ｋ）をｈにより一方向関数演算したたｈ（$h_2^{(2)}$（Ｋ））が与えられる。

【０１１６】

この際、１≦ｔ＜ｃに対して、ｃ＋ｔ番目ユーザは自分のシードキーとh_2（Ｋ）を共に保存する。従って、各ノード毎に合わせてc_2個のキーが加えて保存される。

【０１１７】

前述したように、本発明の変形された第１の実施形態では各ノードに保存されているキー値の数が増加されるが、伝送すべきセッションキーのサイズは減少される。

【０１１８】

図１４は本発明の変形された第１実施形態に係るセッションキー伝送のために区間を分ける方法が図示されている。同図に示すように、多く印加されたユーザ（ｐｒｉｖｉｌｅｇｅｄ　ｕｓｅｒ）らが集まっている場合に、２つの区間１４０１，１４０２のみに分けてセッションキーを伝送することができる。

【０１１９】

図１５は本発明の変形された第１の実施形態に係る多数の区間で分けられた場合セッションキーを伝送する方法が図示されている。同図に示すように、４つの区間１５０１，１５０２、１５０３、１５０４から分けられている場合に、Ｅ（$h^{(2)}$ $h_2^{(2)}$（Ｋ），ＳＫ）のようにセッションキーを構成して伝送することによって、印加されたユーザのみが復号化されることができるよう具現される。

【０１２０】

従って、本発明の変形された第1の実施形態に係るh_2関数を用いることによって計算量を減らし得る。つまり、このときには最大ｃ＋c_2回の一方向関数演算の計算が求められる。

【０１２１】

前述した変形された第１の実施形態によると、ユーザの保存量は基本実施形態に比べてやや増加しているが、除外されたユーザの数が少ない場合にはその伝送量が著しく減少される。

【０１２２】

＜変形された第２の実施形態＞

前述した変形された実施形態における結果として伝送量ｒに近似させた結果を得ることができた。これは今まで知られた方法のうちＳＤの場合に伝送量が２ｒ－１であるのと比較すると、相当改善された結果であることが分かる。後述する変形された第２の実施形態では前記伝送量をｒより減少する方法について提案する。

【０１２３】
変形された第２の実施形態の基本概念は次の通りである。除外されたユーザ（ｒｅｖｏｋｅｄ　ｕｓｅｒ）二人との間に位置しているユーザの集合を区間としてするとき、最悪の場合を考える場合に区間の全体数はｒより小さくはならない。なお、各区間について１回ずつ伝送が行われるので、かかる区間のみを考える場合には伝送量がｒより小さくなることは考えられない。従って、基本的な区間に様々な形の区間を加えなければならない場合が発生する。
【０１２４】
従って、本発明の変形された第２の実施形態では、1つ以上の除外されたユーザを含んでいる区間を加えて伝送区間を設定する。以下、説明では一人の除外されたユーザを含む区間が加えられる例について説明し、同一方法に基づいて二人以上の除外されたユーザを含む区間が加えられる場合も拡張して適用され得る。例えば、合わせて３人の除外されたユーザにより１つの区間が作られるため、理想的にはｒ／２までに伝送量を減らすことができる。
【０１２５】
図１６は本発明の変形された第２の実施形態に係る区間設定の方法を示す図面である。本発明の変形された第２の実施形態では区間内に除外されたユーザを含ませるべく区間を設定することによって、伝送量は減少し、かつ保存量は増大される。つまり、二人の除外されたユーザについて一回にキーを伝送することができるようになる。
【０１２６】
なお、一人の除外されたユーザが加えられた形態については図１６に図示されたように、２つ場合が発生する。前記２つ場合のうち（１）の場合は前述した基本実施形態でその解決が可能であり、（２）の場合には後述する変形された第２の実施形態により効率よく解決できる。
【０１２７】
前記（２）のような区間に対するセッションキーの伝送は次のように行われる。本発明の変形された第２の実施形態により新たな一方向ハッシュ関数であるｇ関数が必要となる。つまり、区間$\{u_i、u_{i+1}、u_{i+2}、\ldots u_{i+S}\}$の除外されたユーザ$u_{i+j}$を含んだ区間であるとする時（尚、全体の区間の長さがｃを超えないと仮定する）、センターは$h^{(s-j)}gh^{(j-2)}(K_i)$を用いてＳＫを暗号化する。
【０１２８】
図１６は一人の除外されたユーザが加えられた形態について説明したが、前述のように複数の除外されたユーザが加えられる場合でも本発明が同一に適用できる。
【０１２９】
図１７は本発明の変形された第２の実施形態に係る線形構造における各ノードにキー値を対応させる方法を示す図面である。同図に示すように、除外されたユーザが出現する前までには１７０１，１７０２，１７０３，１７０４は基本実施形態と同じ一方向キーチェーンに沿って右方向にハッシュ関数ｈを適用し、除外されたユーザu_{i+j}の位置１７０５では一方向ハッシュ関数ｈの代わりに更なる一方向ハッシュ関数であるｇを用いて一方向キーチェーンを変形させる。
【０１３０】
それから、除外されたユーザを通過した後１７０６，１７０７には再度一方向ハッシュ関数ｈを用いてキー値を生成し一方向キーチェーンを作っていく。そして、セッションキーを伝送する際には最後のユーザの位置に該当する値でＳＫを暗号化して伝送する。
【０１３１】
なお、前記２つの一方向関数ｈとｇは全て公開された関数であるので、除外されたユーザの左側に位置するユーザは暗号化に用いられたキーを容易に算出ことができる。しかし、除外されたユーザu_{i+j}は$gh^{(j-1)}(K_i)$の値を把握しなければその後の値の算出を行うことができないので、センタでは$gh^{(j-1)}(K_i)$の値を秘密にする。

【０１３２】
一方、除外されたユーザの右側に位置するユーザの場合にはそれぞれ前記チェーンの中から自分の位置に該当する値を加えて保存していなければならない。なお、区間の長さをｃとして設定する場合、その数を算出してみると、１＋２＋３＋...＋（ｃ－２）となる。つなり、各ユーザは（ｃ－１）（ｃ－２）／２のキーを加えて保存すべきである。
【０１３３】
前述した本発明の変形された第２の実施形態によると、総保存量はｃ＋（ｃ－１）（ｃ－２）／２、即ち、Ｏ（ｃ^{2}）であるが、伝送量はｒ／２＋（Ｎ－２ｒ）／ｃであって、前のｒ部分がｒ／２に減少されたことが分かる。さらに、計算量は基本実施形態のように最大ｃ回の一方向演算の算出となる。
【０１３４】
前述したＮ＝１，０００，０００およびｒ＝５０，０００である場合について算出してみると、下記の表２の結果が獲得される。
【０１３５】
【表２】

Ｃ	保存量	伝送量（ｗｏｒｓｔ　ｃａｓｅ）	ｒａｔｉｏ
６４	１，９５５	２５，０００＋１４，０００	０．７８ｒ
１００	４．９５１	２５，０００＋９，０００	０．６８ｒ

【０１３６】
前記表２によると、伝送量において前のｒ部分はｒ／２に示すように減少したが、後に加えられる（Ｎ－２ｒ）／ｃが大になったことが分かる。
【０１３７】
一方、前述した変形された第２の実施形態の方法は一般的な場合であって、拡張することが可能である。即ち、保存量がＯ（ｃ^{3}）に増加し、三人の除外されたユーザを含んだ区間に一回の伝送でキーを伝送することができるよう具現される。従って、前述したように１つのみならず複数の除外されたユーザを含む区間に対しても適用可能である。
【０１３８】
＜変形された第３の実施形態＞
最後の実施形態として、本発明の変形された第３の実施形態は、前述の変形された第１の実施形態および第２の実施形態を同時に適用した実施形態である。かかる場合、最悪の場合が、長さがｃである区間にて除外されたユーザが一人ずつ含まれている場合である。その理由は、長さがｃより小さい区間に２人以上の除外されたユーザが含まれている場合には前述の変形された第２の実施形態に基づいて除外されたユーザ２人を一回の伝送で解決することができるからである。かかる最悪の場合における伝送量を計算してみると、ｒ／２＋（Ｎ－２ｒ）／２（ｃ－２）であり、保存量はｃ＋ｃ$_{2}$＋（ｃ－１）（ｃ－２）／２である。
【０１３９】
この伝送量に対する式は、ｒがＮ／ｃより大きい場合に適用される。もし、ｒがＮ／ｃより小さければ更なる結果が得られる。例えば、ｒ＝０であれば、必要な伝送量はＮ／（ｃ×ｃ$_{2}$）である。なお、ｒが次第に増大しながら除外されたユーザの含まれた長さｃである区間に対しては一回の伝送が求められ、残り部分に対しては変形された第１の実施形態における方法が適用されるので、大略的にｒ＋（Ｎ－ｃｒ）／（ｃ×ｃ$_{2}$）の伝送量が求められることが分かる。
【０１４０】
即ち、Ｎ／（ｃ×ｃ$_{2}$）を初期値にして勾配が２である直線をなすことになる。同じ方法で、増加した伝送量はｒがＮ／ｃである時点を転換点にして、ｒ／２＋（Ｎ－２ｒ）／２（ｃ－２）の方に変わる。
【０１４１】

前述した変形された第３の形態によると、ユーザの保存量は基本実施形態に比べて多少増加するが、除外されたユーザの数が少ない場合は伝送量が著しく減少する。

【０１４２】

＜変形された第４の実施形態＞

本発明の変形された第４の実施形態は前述した線形構造における基本実施形態および変形された第１実施形態ないし変形された第３の実施形態を環状構造で適用した方法である。

【０１４３】

最初に、前述した実施形態での線形構造（ｓｔｒａｉｇｈｔ　ｌｉｎｅ　ｓｔｒｕｃｔｕｒｅ）を環状構造で容易に再構成することができる。即ち、u_1からu_NまでのＮ名のユーザを有する直線Ｌを考慮する際に、前記Ｌの２つの終り点を連結させると前記直線は環状となる。

【０１４４】

前記環状から予め設定された区間に対して、前述した基本実施形態のような全ての一方向キーチェーン方法が適用され得る。例えば、ユーザu_Nノードから開始される一方向キーチェーンが構成されるのである。

【０１４５】

前記線形構造を有する基本実施形態では、前記ユーザu_Nノードから開始される一方向キーチェーンは$K_{N,\ N}$の１つのキーを有する。一方、本発明の変形された第４の実施形態に係る環状構造では前記u_Nとu_1を連結して引き続き一方向キーチェーンを形成するので、ユーザu_Nノードから開始される一方向キーチェーンは下記の数３のようなｃ個のキー値を有する。

【０１４６】

【数３】

$$K_{N,\ N},\ K_{N,1},\ K_{N,2},\ K_{N,3},\ \cdots,\ K_{N,c-1}$$

【０１４７】

これを一般化してu_iノードから開始される一方向キーチェーンを次の数４のように表すことができる。

【０１４８】

【数４】

$$K_{i,i},\ K_{i,\ i+1(\mathrm{mod}N)},\ \cdots,\ K_{i,i+c-1(\mathrm{mod}N)}$$

【０１４９】

即ち、変形された第４の実施形態の場合、連続した正当ユーザからなる区間の最大長さをｃとすると、線形構造ではそれぞれのユーザの位置に応じて１からｃ個までのキーが保存されるが、環状構造ではそれぞれのユーザはそれぞれｃ個のキーが保存されるべきである。

【０１５０】

図１８は本発明の変形された第４の実施形態に係る環状の各ノードにキー値の対応された結果を表した図面である。同図に示すように、変形された第４の実施形態では、環状グループを構成しているノードが１０個であり、連続した正当なユーザから構成された区間の最大長さが５個である場合に、各ノードが５個のキーを保存していることが確認できる。

【０１５１】

これによって、環状構造においても前述した変形された第１の実施形態における区間の長さをｃと設定することによって伝送量がｒより大になることを補完するために、長い区間について一回の伝送のみでキー値を伝送できる方法が適用可能である。それと共に、環

状構造においても前述した変形された第２の実施形態における伝送量をｒより減少させるために、除外されたユーザの位置から新たな一方向関数を適用する方法が適用可能であり、さらに、前述した変形された第３の実施形態における変形された第１の実施形態および変形された第２の実施形態の組み合わせた方法に基づいてもその適用が可能となる。

【０１５２】

＜変形された第５の実施形態＞

本発明の変形された第５の実施形態は階層構造を有する環状構造を提案する。

【０１５３】

図１９は本発明の一実施の形態に係る環状構造のノードグループの階層構造を示している。

【０１５４】

同図を参照すると、階層構造上の各環状構造のノードグループはｃ個のノードからなっている。このときに、各ユーザは前記階層構造の全てのノード（即ち、環状構造）における各点に対応する。もし、前記階層構造がルーツノードを除いて１６階層から構成されていれば、前記階層構造ではｃ^{16}のユーザを対応することができるようになる。

【０１５５】

従って、各階層でのグループノード別に前述したようなキーチェーンを有する環状構造が構成されることができる。このとき、前記各ノードに対応するユーザは自分の親ノードに割り当てられた全てのキー値を有するようになる。

【０１５６】

前記構造から、少なくとも１つの除外されたユーザを含んでいる子ノードを有する各ノードは、除外されたノードとして見なされる。従って、暗号化する際に、まずセンタでは前記除外されたノードを表示する。それから、前記センタでは前記除外されたノードの親ノードを階層構造に従って表示していく。

【０１５７】

かかる過程がルーツノードまで完了され、もし、少なくとも１つの除外されたノードがあればルーツノードは除外されたノードとなる。

【０１５８】

前記除外されたノードを確認してから、センタでは各階層における区間を設定する。図示されたように第０階層の上では１つのノードのみが含まれる。

【０１５９】

最初に、センタでは第０階層の環状グループから循環区間を設定し、前記設定された各循環区間に対して区間キーとしてセッションキーを暗号化する。それから、センタでは第１階層について前記第０階層で除外されたノードの子ノードに該当する環状グループのみを考慮する。前述のような過程は第１５階層までに進行される。

【０１６０】

例えば、１つの除外されたユーザを有す場合、前記表示する過程にて全ての階層から１つの除外されたノードが発生されるようになる。さらに、暗号化ステップにては第０階層にて１つの除外されたノードがあることから、前記センタでは１つのノードを除外した循環区間に対する区間キーとしてセッションキーが暗号化される。一方、第１階層についてセンタは前記第０階層での除外されたノードの子ノードに該当する１つの環状グループのみを考慮する。

【０１６１】

認証されたノードの子ノードに該当する環状グループを構成している各ノードは前記自分の親ノードから与えられアセッションキーを得ることができる。結果的にはセンタでは１６回暗号化することによって、全体の階層構造に対する暗号化の処理を行うことができる。

【０１６２】

前述した変形された第４の実施形態では、前の実施形態より数多いユーザに対する暗号化処理を行うことができる一方、より多いキーが求められるようになる。しかし、前述の

第２の実施形態よりも伝送オーバーヘッド（ＴＯ）を著しく減少させることができる。

【０１６３】

即ち、変形された第４の実施形態の階層をｋ階層とし、各環状グループに含まれたノードの個数をそれぞれｃ個とすると、前記変形された第４の実施形態にて各ユーザの保存オーバーヘッドはｋｃ＋（ｃ－１）（ｃ－２）／２であって、（ｋ－１）ｃ個のキーが増加する。

【０１６４】

一方、伝送オーバーヘッドはc^{k-1}／２＜ｒである場合、約ｒ／２＋３Ｎ／４ｃとなる。これはｒ＜Ｎ／６である場合、前記変形された第４の実施形態が前述した変形された第２の実施形態よりも少ない伝送オーバーヘッドを有していることが分かる。

【０１６５】

また、前の説明では１つの除外されたユーザを含んでいる区間（１－ｐｕｎｃｔｕｒｅｄ）について適用しているが、前記変形された第２の実施形態では前述のように複数の除外されたユーザを含んでいる区間（ｐ－ｐｕｎｃｔｕｒｅｄ）についても適用できることは自明である。さらに、前述の階層構造におけるより多い階層に対しても前記除外されたユーザに対する区間設定および伝送方法を使用することができる。

【０１６６】

以上、本発明に係る各実施形態について説明したが、この実施形態がブロードキャスト暗号化に実際適用されることにあたって、全てのユーザがシステムの初期に同時加入することは難しい。つまり、センタは将来に加えられるユーザのために、予めキーを設定しておくべきであるが、このようなキーは基本的に除外された状態として維持されなければならない。そうでなければ、新たに加入したユーザが過去に伝達されたメッセージを復旧する恐れがあるからである。

【０１６７】

ほとんどのブロードキャスト暗号化の場合、伝送量がｒに依存することを考えると、これはセンタに大きい負担になりかねない。従って、新たなユーザのキーを予め作らずに後で追加する機能というのは極めて重要である。前記で提案された実施形態はいつでも新たなユーザが追加されるたびに直線の右側に新たなノードを追加すれば容易に解決される。このときに、計算量は、新たなランダム値を選択すること、一方向関数の演算を数回程度行うことが加えられるので、効率よくユーザの追加を行うことができる。勿論、他のユーザのキーにいずれの影響も及ぼさない。

【０１６８】

一方、ユーザの代替側面からみると、これはシステムが長時間の間に使用された後のメンテナンスに関わりがある。システムが長時間維持された場合に、永久的に除外されたユーザは常に除外されたままの状態であるため、伝送量がｒに依存するほとんどの方法において伝送量を増加させてしまう、という大きな要因に繋がる。

【０１６９】

かかる場合に、永久除外されたユーザのキーを取り除いた後、新たなユーザをその位置に加えることで除外されたユーザの数を減少させる必要がある。従来の補間などの方法では、このようなユーザ代替が割合自在に実行され得るものの、階層などの構造を用いた方法によると難しい作業である。ＳＤの場合は、一人のユーザを代替するために、ルーツノードのキーを新たに変えなければならないので、全てのユーザのキーを更新せざるを得ない不都合がある。

【０１７０】

一方、前述した本発明に係る実施形態では、前記ＳＤなどのツリーを用いた方法よりも比較的に容易に適用できる。つまり、一人のユーザを代替したい場合は基本実施形態の場合、合わせて２ｃ名のユーザのキーを更新すればよい。

【０１７１】

謀反人（ｔｒａｉｔｏｒ）は、正当なユーザの中で自分の暗証キーを流出し不法的なユーザにメッセージを見せるよう手伝うユーザである。謀反人追跡は、このような不法なユ

ーザが存在する場合、彼らが有しているキーからキーを流出させたユーザを探し出すアルゴリズムのことをいう。

【０１７２】

かかる謀反人追跡に対する結果は色々であるが、各ユーザのキーが全て区別可能であり、多数のユーザのキーから新たなキーを生成することができない場合は基本的に謀反人追跡が可能であると知られている。一方、前提案された本発明の実施形態は、かかる性質を満足させるため、謀反人の追跡が可能になる。

【０１７３】

また、基本実施形態を、公開キーを利用する方式に変形することで、各ユーザの暗証キーを２つに減らすことができる。この場合に、必要な公開キーはＯ（ｃ^{2}）となる。かかる変形は公開キーのサイズが制限的ではない応用分野において使用するとき有用である。

【０１７４】

結論的に、様々なブロードキャスト暗号化方法のうち現在最も効果的なＣＳおよびＳＣ方法と本発明との比較結果が下記の表３に表れている。なお、前述した結果のようにＮ＝１，０００，０００及びｒ＝５０，０００である場合である。

【０１７５】

【表３】

	Ｃ	Ｃ2	保存量	伝送量（worst case）
基本実施形態	200		200（2K）	50,000+4,500(1.1r)
変形された第2の実施形態	64		1,955	25,000+14,000(0.78r)
変形された第3の実施形態	64	20	1,955	25,000+7,260(0.64r)
変形された第4の実施形態	100	100	5,151	25,000+4,500(0.59r)
ＣＳ			20	r×(log(N/r)(4r)
ＳＤ			200	100,000(2r)

【０１７６】

上記の表３を参照すると、本発明の実施形態に基づくとブロードキャスト暗号化で最も重要な伝送量がｒ未満に減ることが分かる。つまり、本発明の実施形態は今まで最も好ましい方法であると知られているＳＤと比較して伝送量が著しく減ったことが分かる。また、前述した実際の適用に必要な様々な特性をも含んでいる。

【０１７７】

以上、図面に基づいて本発明の好適な実施形態を図示および説明してきたが本発明の保護範囲は、前述の実施形態に限定するものではなく、特許請求の範囲に記載された発明とその均等物にまで及ぶものである。

【産業上の利用可能性】

【０１７８】

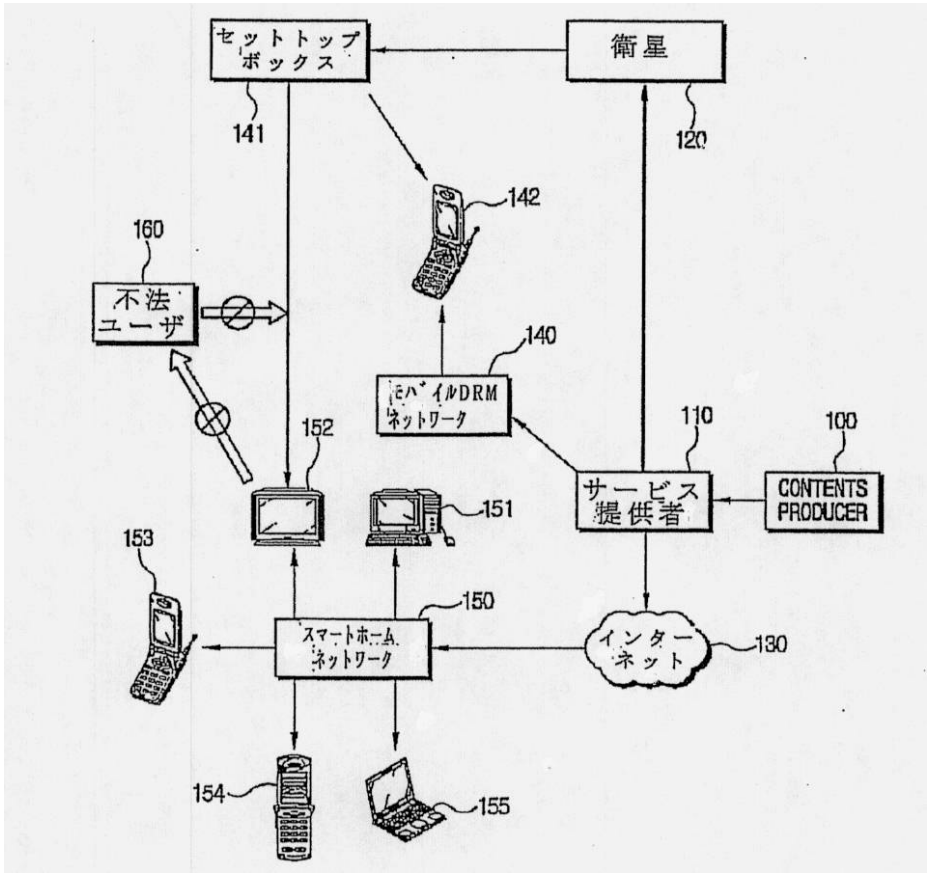
本発明はブロードキャスト暗号化のような暗号化に用いられる。

【符号の説明】

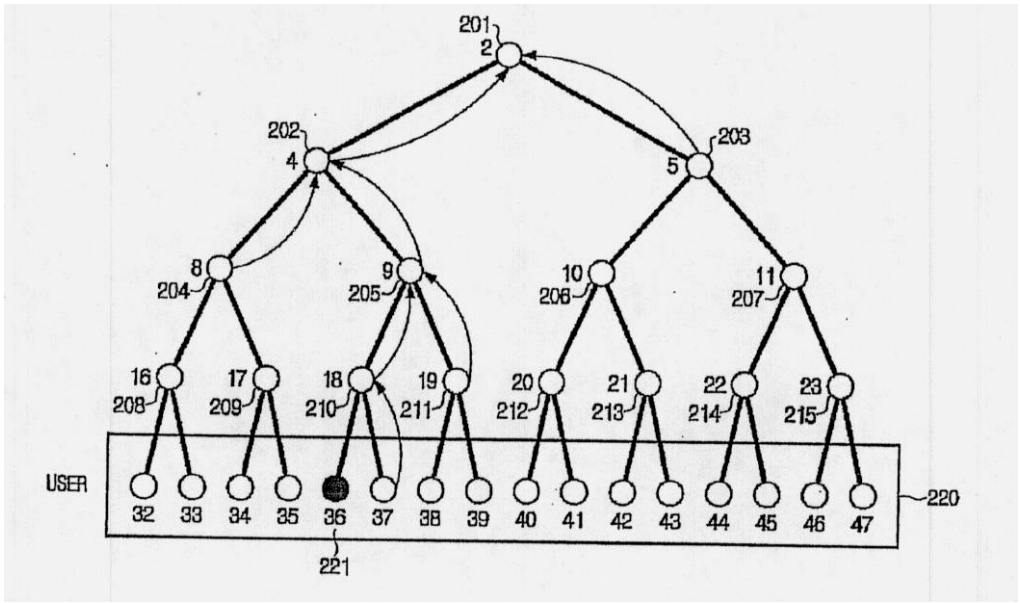
【０１７９】

１００　コンテンツ生産者
１１０　サービス提供者
１２０　衛星
１３０　インタネットネットワーク
１４０　ネットワーク
１４１　セットトップボックス
１４２　移動通信端末
１５０　スマートホームネットワーク
１５１，１５２，１５３，１５４，１５５　端末
１６０　不法ユーザ

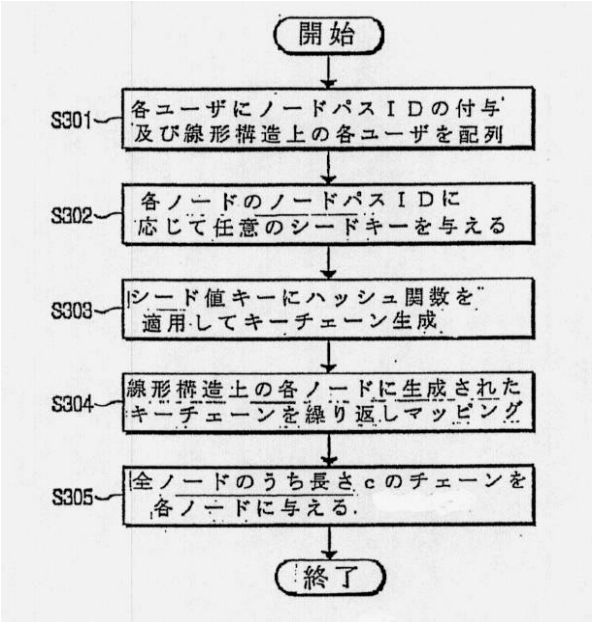
【図１】


セットトップボックス
衛星
141
120
142
160
不法ユーザ
140
モバイルDRMネットワーク
110
100
152
サービス提供者
CONTENTS PRODUCER
151
153
150
スマートホームネットワーク
インターネット
130
154
155

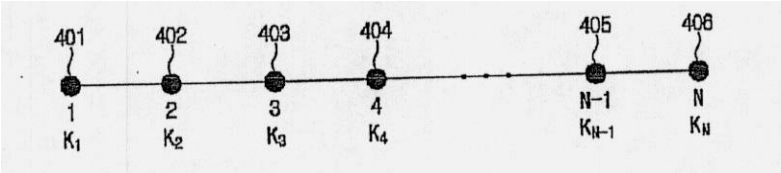
【図２】


201
2
202
4
203
5
8
204
9
205
10
206
11
207
16
208
17
209
18
210
19
211
20
212
21
213
22
214
23
215
USER
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
220
221

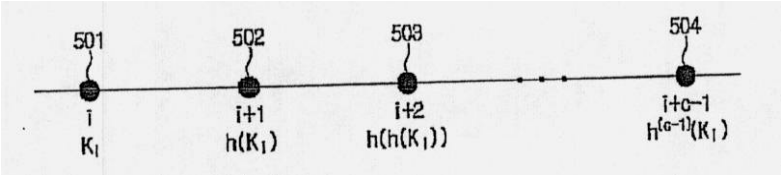
【図３】


開始
S301
各ユーザにノードパスＩＤの付与及び線形構造上の各ユーザを配列
S302
各ノードのノードパスＩＤに応じて任意のシードキーを与える
S303
シード値キーにハッシュ関数を適用してキーチェーン生成
S304
線形構造上の各ノードに生成されたキーチェーンを繰り返しマッピング
S305
全ノードのうち長さｃのチェーンを各ノードに与える.
終了

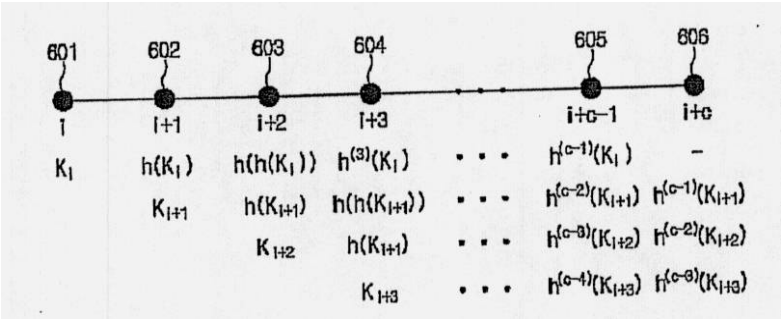
【図４】


401
402
403
404
405
406
1
K1
2
K2
3
K3
4
K4
N-1
KN-1
N
KN

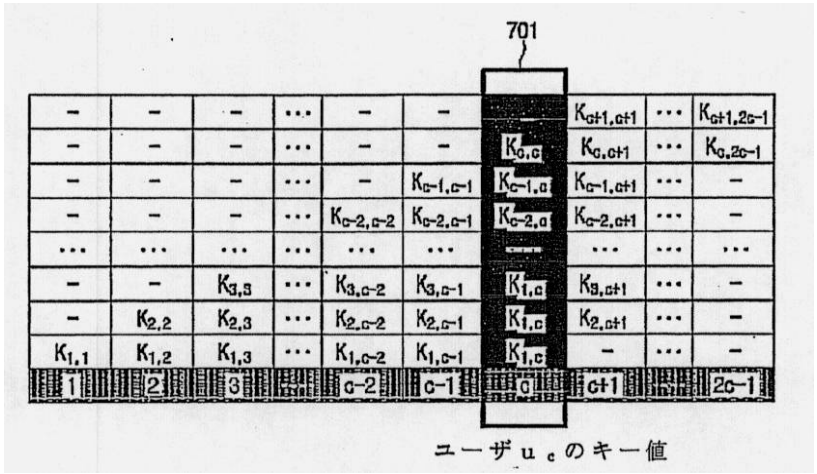
【図５】


501
502
503
504
i
Ki
i+1
h(Ki)
i+2
h(h(Ki))
i+c-1
h^(c-1)(Ki)

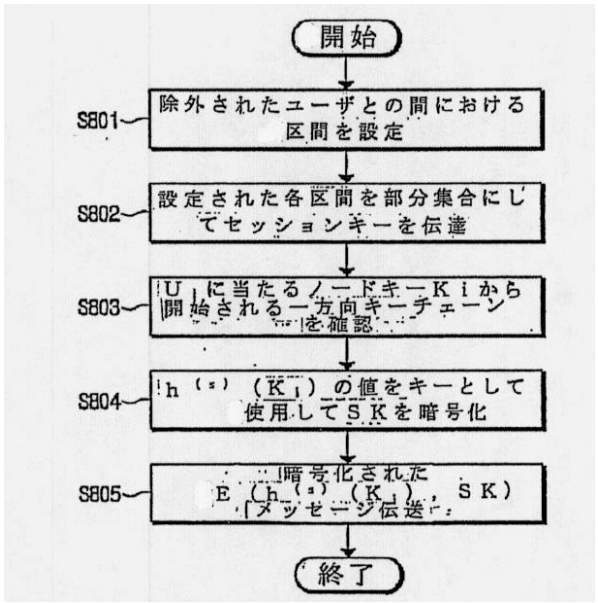
【図６】


601
602
603
604
605
606
i
Ki
i+1
h(Ki)
Ki+1
i+2
h(h(Ki))
h(Ki+1)
Ki+2
i+3
h(3)(Ki)
h(h(Ki+1))
h(Ki+1)
Ki+3
i+c-1
h^(c-1)(Ki)
h^(c-2)(Ki+1)
h^(c-3)(Ki+2)
h^(c-4)(Ki+3)
i+c
-
h^(c-1)(Ki+1)
h^(c-2)(Ki+2)
h^(c-3)(Ki+3)

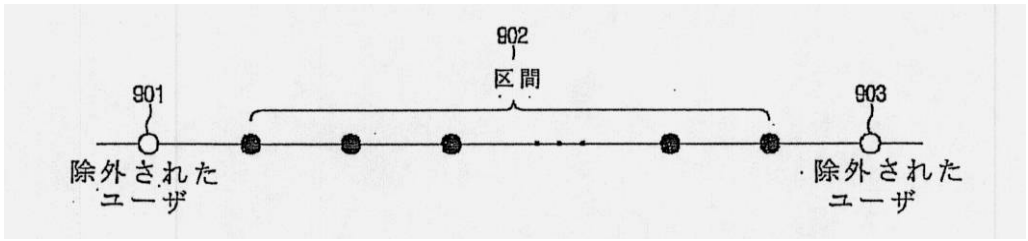
【図７】


701
ユーザｕｃのキー値

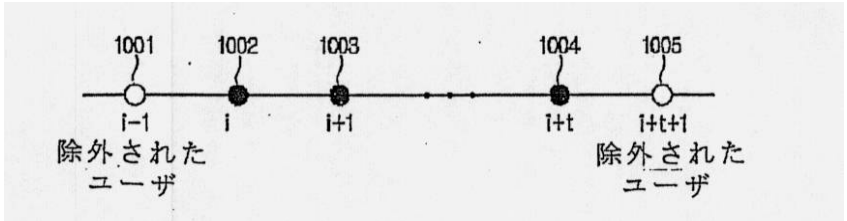
【図８】


開始
S801
除外されたユーザとの間における区間を設定
S802
設定された各区間を部分集合にしてセッションキーを伝達
S803
Ｕｉに当たるノードキーＫｉから開始される一方向キーチェーンを確認
S804
ｈ（＝）（Ｋｉ）の値をキーとして使用してＳＫを暗号化
S805
暗号化された
Ｅ（ｈ（＝）（Ｋｉ），ＳＫ）
をメッセージ伝送
終了

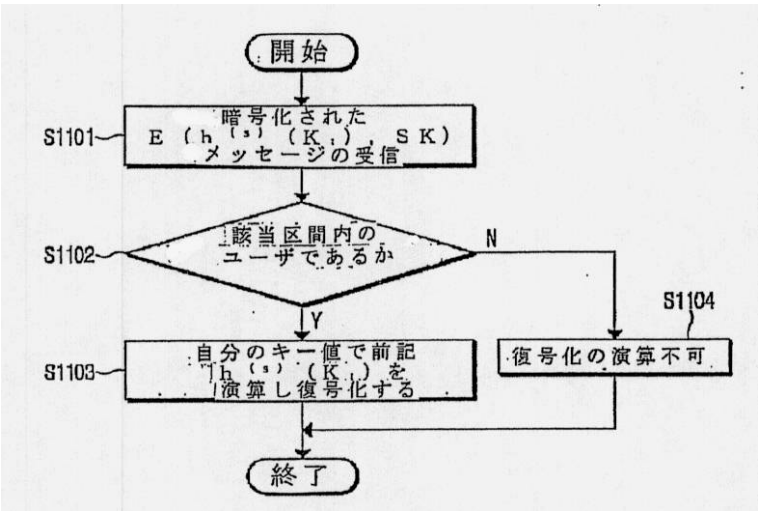
【図９】


902
区間
901
903
除外されたユーザ
除外されたユーザ

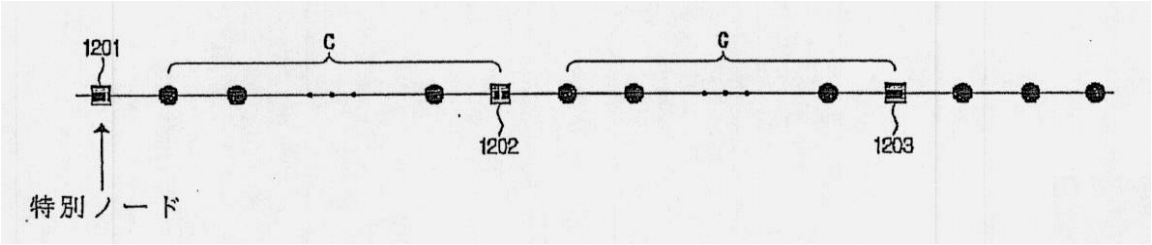
【図１０】


1001
1002
1003
1004
1005
i-1
i
i+1
i+t
i+t+1
除外されたユーザ
除外されたユーザ

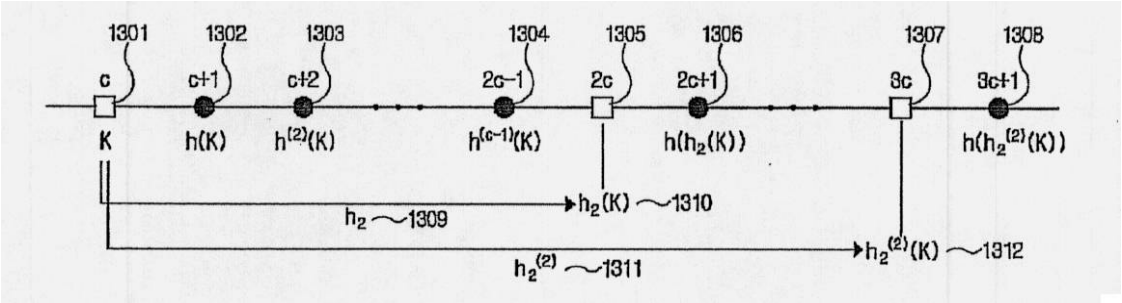
【図１１】



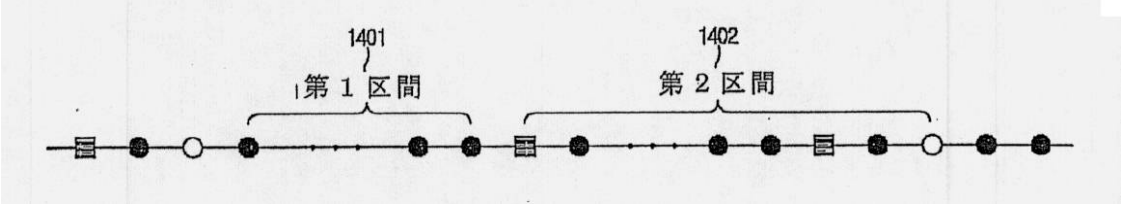
【図１２】



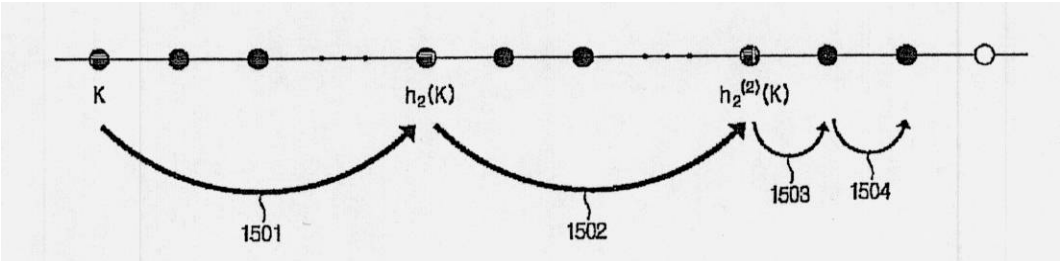
【図１３】



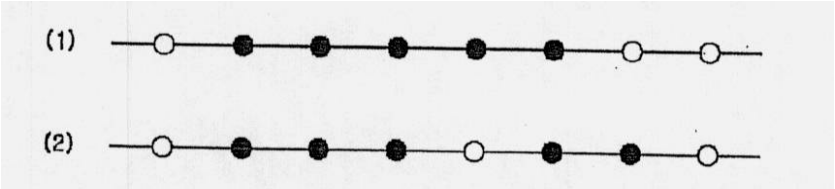
【図１４】



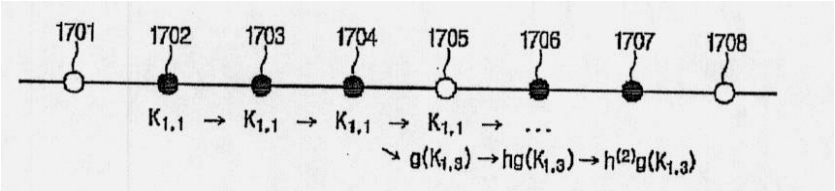
【図１５】



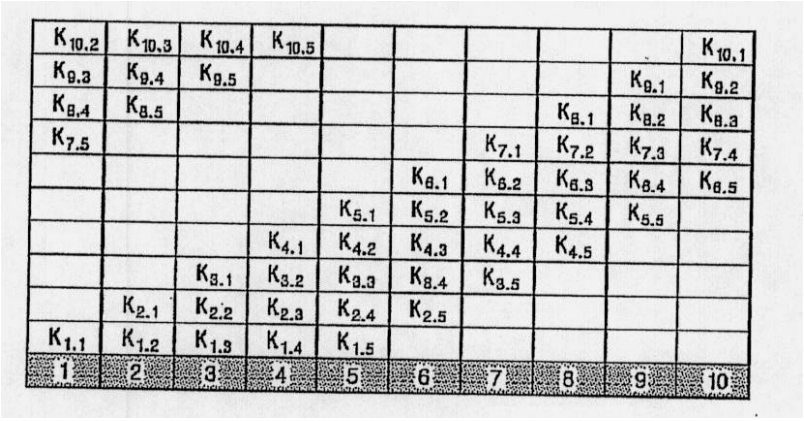
【図１６】



【図１７】

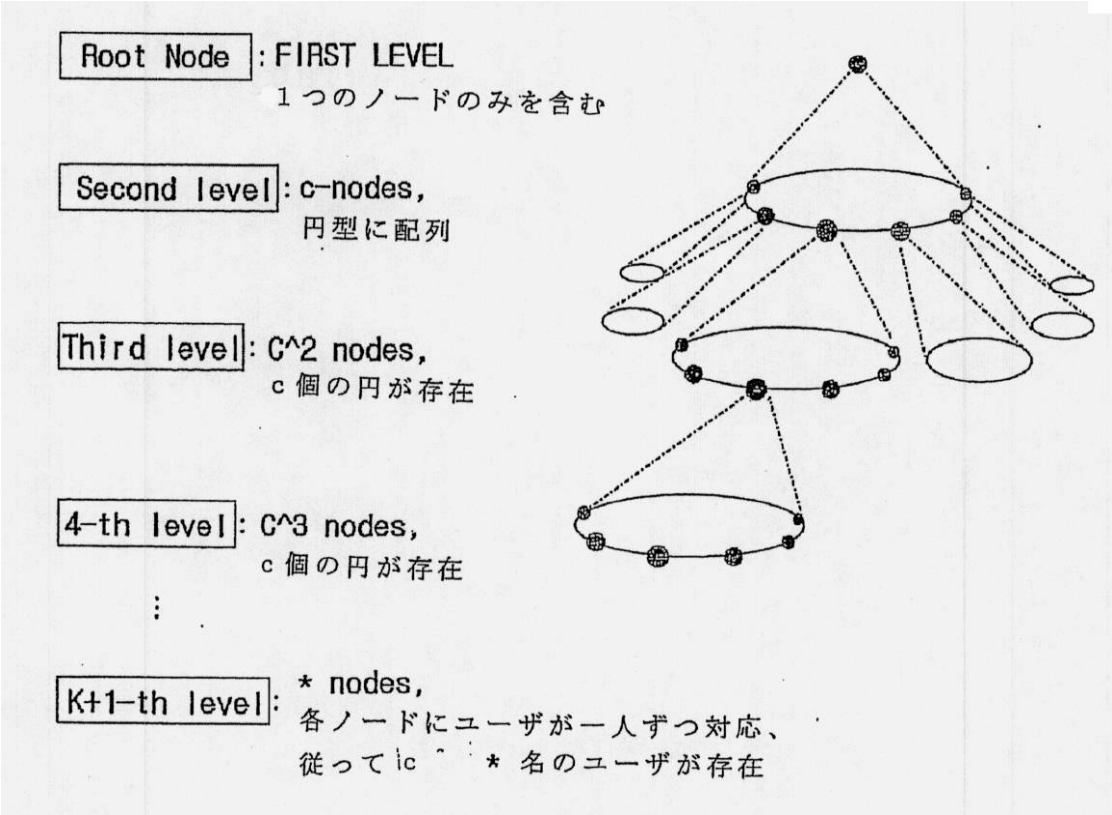


【図１８】



$K_{10,2}$	$K_{10,3}$	$K_{10,4}$	$K_{10,5}$						$K_{10,1}$
$K_{9,3}$	$K_{9,4}$	$K_{9,5}$						$K_{9,1}$	$K_{9,2}$
$K_{8,4}$	$K_{8,5}$						$K_{8,1}$	$K_{8,2}$	$K_{8,3}$
$K_{7,5}$						$K_{7,1}$	$K_{7,2}$	$K_{7,3}$	$K_{7,4}$
					$K_{6,1}$	$K_{6,2}$	$K_{6,3}$	$K_{6,4}$	$K_{6,5}$
				$K_{5,1}$	$K_{5,2}$	$K_{5,3}$	$K_{5,4}$	$K_{5,5}$	
			$K_{4,1}$	$K_{4,2}$	$K_{4,3}$	$K_{4,4}$	$K_{4,5}$		
		$K_{3,1}$	$K_{3,2}$	$K_{3,3}$	$K_{3,4}$	$K_{3,5}$			
	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$	$K_{2,4}$	$K_{2,5}$				
$K_{1,1}$	$K_{1,2}$	$K_{1,3}$	$K_{1,4}$	$K_{1,5}$					
1	2	3	4	5	6	7	8	9	10

【図１９】



フロントページの続き

(72)発明者　ウェオン－イル・ジン
大韓民国・ギョンギ－ド・４４０－７１９・スウォン－シ・ジュンガン－グ・ジョンジャ－ドン・８８０－３・ベクソル－マウル・ジンロ・アパートメント・５２６－１９０３
(72)発明者　ファン－ジョーン・キム
大韓民国・ソウル・１３３－７７５・ソンドン－グ・ヘンダン・２－ドン・（番地なし）・デリム・アパートメント・１５３－１０２
(72)発明者　スン－ジョーン・パク
大韓民国・ソウル・１５６－０９０・ドンジャク－グ・サダン－ドン・５７－１８・１４－７
(72)発明者　ジュン－ヒー・チョン
大韓民国・ソウル・１５１－８１８・グワナク－グ・ボンチョン・７－ドン・２４４－２・プロフェッサーズ・アパートメント・オブ・ソウル・ナショナル・ユニバーシティ・ガ－５０４
(72)発明者　ミュン－ファン・キム
大韓民国・ソウル・１５１－７５２・グワナク－グ・ボンチョン・１－ドン・（番地なし）・ボラメ・サムスン・アパートメント・１０７－１３０４
(72)発明者　ナム－ス・ジョ
大韓民国・ソウル・１５１－８５８・グワナク－グ・シリム・９－ドン・２２０－１２・５０４
(72)発明者　エン－スン・ヨー
大韓民国・ギョンギ－ド・４７２－７９５・ナムヤンジュ－シ・ドノン－ドン・（番地なし）・ブヨン・アパートメント・５１０－４０１

Ｆターム(参考) 5J104 AA16 AA32 EA06 EA18 JA03 MA05 NA02 NA36 NA37 PA01