

(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
2010 年 6 月 17 日(17.06.2010)

PCT

(10) 国際公開番号
WO 2010/067650 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) H04L 12/56 (2006.01)
H04L 9/16 (2006.01) H04W 12/02 (2009.01)
- (21) 国際出願番号: PCT/JP2009/065664
- (22) 国際出願日: 2009 年 9 月 8 日(08.09.2009)
- (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 2008-313346 2008 年 12 月 9 日(09.12.2008) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社東芝 (Kabushiki Kaisha Toshiba) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 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): 大熊 建司 (OHKUMA, Kenji) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 松下 達之 (MATSUSHITA, Tatsuyuki) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 山中 晋爾 (YAMANAKA, Shinji) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1

号 株式会社東芝 知的財産部内 Tokyo (JP). 村谷 博文 (MURATANI, Hirofumi) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 花谷 嘉一 (HANATANI, Yoshikazu) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 磯谷 泰知 (ISOGAI, Taichi) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 米村 智子 (YONEMURA, Tomoko) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP). 古田 憲一郎 (FURUTA, Kenichiro) [JP/JP]; 〒1058001 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝 知的財産部内 Tokyo (JP).

(74) 代理人: 酒井 宏明, 外 (SAKAI, Hiroaki et al.); 〒1006020 東京都千代田区霞が関三丁目 2 番 5 号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).

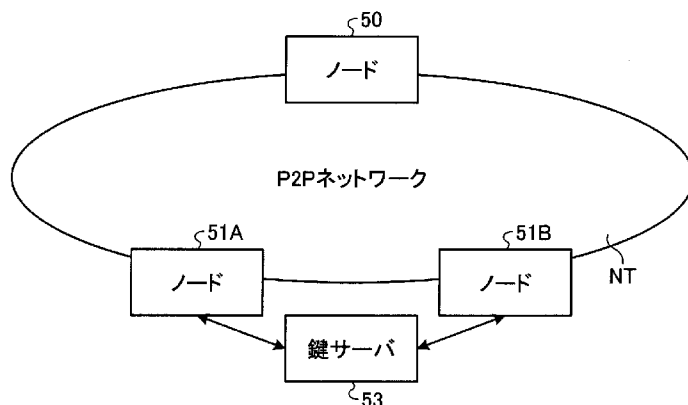
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS,

[続葉有]

(54) Title: COMMUNICATION DEVICE, SERVER, COMMUNICATION METHOD, PROGRAM

(54) 発明の名称: 通信装置、サーバ、通信方法及びプログラム

[図1]



50 NODE
NT P2P NETWORK
51A NODE
51B NODE
53 KEY SERVER

(57) Abstract: A communication device which transmits a piece as a part of data receives: a first piece which has been reversibly converted by other communication device; a first device identifier allocated to the other communication device; and first temporary information generated by the other communication device. The communication device stores the first device identifier while correlating the first piece, the identifier, and the first temporary information to each other and stores a second device identifier allocated to the communication device. The communication device generates second temporary information which may differ in each generation, converts the first piece by using the second temporary information, and outputs the second piece. The communication device transmits the second piece, the first device identifier, the second device identifier, the first temporary information, and the second temporary information.

(57) 要約: データの一部であるピースを送信する通信装置は、他の通信装置によって可逆に変換された第1ピースと、当該他の通信装置に割り当てられた第1装置識別情報とを受信し、第1ピースと、第1装置識別情報と、第1一時情報とを対応付けて記憶し、当該通信装置に割り当てられた第2装置識別情報を生成し、第2一時情報を生成し、第2一時情報を用いて、第1ピースを変換して、第2ピースを出力し、第2ピースと、第1装置識別情報と、第2装置識別情報と、第1一時情報と、第2一時情報とを送信する。

れた第1装置識別情報と、当該他の通信装置によって生成された第1一時情報とを受信し、第1ピースと、第1装置識別情報と、第1一時情報とを対応付けて記憶し、当該通信装置に割り当てられた第2装置識別情報を生成し、第2一時情報を生成し、第2一時情報を用いて、第1ピースを変換して、第2ピースを出力し、第2ピースと、第1装置識別情報と、第2装置識別情報と、第1一時情報と、第2一時情報とを送信する。

WO 2010/067650 A1



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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- (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, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,

- 国際調査報告 (条約第 21 条(3))
- 補正された請求の範囲及び説明書 (条約第 19 条(1))

明 細 書

発明の名称 : 通信装置、サーバ、通信方法及びプログラム

技術分野

[0001] 本発明は、通信装置、サーバ、通信方法及びプログラムに関する。

背景技術

[0002] 例えば、P2P(peer to peer)を利用してデータを配信する配信方式（P2P配信という）は、巨大なストレージと大きな通信帯域とを有するデータ配信サーバを必要とせず、コストメリットの大きい配信方式である。また、データの配信を受けるノードにおいては、複数のノードからのデータの供給が期待されるため、ダウンロードやアップロードにおける帯域幅を活かした高速なデータ取得が期待される。このようにP2Pデータ配信には大きなメリットがあるが、一方で、著作権保護などデータセキュリティの観点から安全性に不安があった。P2P配信に限らず、著作権保護などのデータセキュリティを考える上で一般的な前提として次のことを仮定する。全ての端末機器又はノードがハッキングされることはないということである。この前提を否定した場合、端末機器は秘密とすべきデータを保持したり、秘密とすべき処理を行ったりすることができなくなり、殆どのセキュリティ技術やセキュリティ確保の為の工夫が成立しない。

[0003] さて、P2P配信において、暗号化されたデータを配信し、データの配信を受けるノードが当該データ（配信データという）を復号するための復号鍵を取得するコンテンツ配信システムがある。このようなシステムのP2P配信においてデータセキュリティ上の大きな問題点は、配信データと当該配信データを復号するための復号鍵との組み合わせが単一であったり数が少なかったりすることである。この場合、あるノードがハッキングされ、復号鍵が暴露されたとする。この場合、この復号鍵は殆どの配信データを復号するために使用できることになる。この問題を解決する方法の一つの方法は、配信データをノード毎に個別化することである。

[0004] P2P配信において配信データをノード毎に個別化する技術としては、例えば、特許文献1に示されるMarkingの方式が知られている。この方式では、配信データをピースに分割した上で、鍵の行列で暗号化を施して暗号化ピースを生成する。その結果として、行列状に暗号化された暗号化ピースからなるピース群が生成される。そしてこのようなピース群はP2Pネットワークを介して配信される。当該P2Pネットワークに接続される1つのノードは、各ピースについて行列状に暗号化された複数の暗号化ピースの中から1つの暗号化ピースを取得することになる。結果として、配信データを構成する各ピースが各々暗号化された暗号化ピースの組み合わせは、ノード毎に統計的に一意になることが期待される。

先行技術文献

特許文献

[0005] 特許文献1：USP 7165050

発明の概要

発明が解決しようとする課題

[0006] しかし、上述の特許文献1の技術においては、各暗号化ピースの組み合わせがノード毎に一意であることはあくまで統計的に期待されるだけである。各暗号化ピースの組み合わせをノード毎に一意にすることを実現するには、例えば、以下の2つの方法が考えられる。1つは、暗号化ピースの配信方法に工夫を施すという方法である。また、1つは、各暗号化ピースを復号するための復号鍵を保持する鍵サーバが復号鍵の配信を制限するという方法である。例えば、配信されたピース群をノードは復号するために、各暗号化ピースの組み合わせを鍵サーバに申告して復号鍵を取得するシステムがある。このシステムにおいて、復号鍵の再配信によるリプレイアタックを阻止するためには、既に取得された復号鍵と重複が多い暗号化ピースの組み合わせを、鍵サーバがリジェクトするという方法がある。しかしいずれの方法であっても、暗号化ピースの配信効率を時として著しく低下させ、P2Pネットワー

クの利点を十分活かすことができなくなる恐れがある。また、前者の方法では、データの保護とデータの配信方法との独立性が損なわれ、そのことがシステム構築上の大きな制約となる恐れがある。

[0007] 本発明は、上記に鑑みてなされたものであって、コンテンツ配信システムにおいて配信される各ピースの組み合わせを通信装置毎に一意にすることが可能になると共に、システム構築上の自由度を向上可能であり、通信装置における計算の効率を向上可能な通信装置、サーバ、通信方法及びプログラムを提供することを目的とする。

課題を解決するための手段

[0008] 上述した課題を解決し、本発明は、データの一部であるピースを送信する通信装置であって、他の通信装置によって可逆に変換された第1ピースと、当該他の通信装置に割り当てられた第1装置識別情報と、当該他の通信装置によって生成された第1一時情報とを受信する受信手段と、前記第1ピースと、前記第1装置識別情報と、前記第1一時情報とを対応付けて記憶する第1記憶手段と、当該通信装置に割り当てられた第2装置識別情報を記憶する第2記憶手段と、その生成毎に異なり得る第2一時情報を生成する第1生成手段と、前記第2一時情報を用いて、前記第1ピースを変換して、第2ピースを出力する変換手段と、前記第2ピースと、前記第1装置識別情報と、前記第2装置識別情報と、前記第1一時情報と、前記第2一時情報とを送信する送信手段とを備えることを特徴とする。

[0009] また、本発明は、データの一部であるピースを受信する通信装置であって、当該通信装置に割り当てられている装置識別情報を記憶する第1記憶手段と、他の通信装置によって可逆に変換されたピースと、当該他の通信装置に割り当てられている装置識別情報と、当該他の通信装置によって生成された一時情報とを受信する第1受信手段と、前記ピース、前記装置識別情報及び前記一時情報を対応付けて記憶する第2記憶手段と、前記ピースを逆変換するための復号情報を要求すると共に、当該ピースと対応付けられて記憶された前記装置識別情報及び前記一時情報を対応付けて含む要求を鍵サーバへ送

信する送信手段と、前記要求に応じて前記鍵サーバから、前記復号情報を受信する第2受信手段と、受信された前記復号情報を用いて前記ピースを復号する復号手段とを備えることを特徴とする。

- [0010] また、本発明は、サーバであって、データの一部であるピースを送信する複数の他の通信装置のそれぞれに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶する第1記憶手段と、可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第1通信装置から受信する受信手段と、前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する第1生成手段と、前記変換パラメータを含む前記復号情報を前記第1通信装置に送信する送信手段とを備えることを特徴とする。

発明の効果

- [0011] 本発明によれば、コンテンツ配信システムにおいて配信される各ピースの組み合わせを通信装置毎に一意にすることが可能になると共に、システム構築上の自由度を向上可能であり、通信装置における計算の効率を向上可能になる。

図面の簡単な説明

- [0012] [図1]第1の実施の形態にかかるデータ配信システムの構成を示す図。
[図2]ノード50の機能的構成を例示する図。
[図3]ノード51の機能的構成を例示する図。
[図4]ノード50からノード51Aに送信される情報を模式的に示す図。
[図5]ノード51Aからノード51Bに送信される情報を模式的に示す図。
[図6]ノード51Bから鍵サーバに送信される情報を模式的に示す図。
[図7]鍵サーバ53からノード51Bに送信される復号情報を模式的に示す図

。

[図8] 鍵サーバ53の機能的構成を例示する図。

[図9] ノード50が行う配信処理の手順を示すフローチャート。

[図10] ノード51が暗号化ピースを受信する受信処理の手順を示すフローチャート。

[図11] ノードに受信される情報を模式的に示す図。

[図12] 配信開始ノード以外のノード51が行う配信処理の手順を示すフローチャート。

[図13] ノードが送信する情報を模式的に示す図。

[図14] ノード51が暗号化ピースを復号する復号処理の手順を示すフローチャート。

[図15] ノードが送信する情報を模式的に示す図。

[図16] ノードが受信する対称鍵を模式的に示す図。

[図17] 鍵サーバ53がノード51からの鍵要求に応じて復号情報を送信する復号情報送信処理の手順を示すフローチャート。

発明を実施するための形態

[0013] 以下に添付図面を参照して、この発明にかかる通信装置、サーバ、通信方法及びプログラムの一実施の形態を詳細に説明する。

[0014] 図1は、本実施の形態にかかるデータ配信システムの構成を示す図である。本実施の形態にかかるデータ配信システムにおいては、複数のノード50、51A～51BがP2PネットワークNTを介して接続されている。図示しないがこの他のノードもP2PネットワークNTを介して接続され得る。また、各ノード50、51A～51Bは鍵サーバ53と接続されている。各ノード50、51A～51Bは、各ノードに一意に割り当てられた装置識別情報であるノードIDと、各ノードに一意に割り当てられた割当情報として秘密鍵を保持している。各ノード50、51A～51Bに割り当てられたノードIDを各々ID#0、ID#1、ID#2とし、秘密鍵を各々 s_0 、 s_1 、 s_2 とする。尚、各ノード50、51A～51Bのうちノード50は、データの配信の基点となる

配信開始ノードであり、配信対象のデータ（配信データという）を保持している。配信データは、平文である場合も既に暗号化された暗号文である場合もある。例えば、当該配信データは、暗号化として何らかのDRM（Digital Right Management）Systemによって保護されたビデオデータであっても良い。鍵サーバ53は、各ノード50、51A～51Bに各々割り当てられた秘密鍵を保持している。尚、以降、ノード51A～51Bを各々区別する必要がない場合、単にノード51と記載する。

[0015] ここで、各ノード50、51と、鍵サーバ53との各装置のハードウェア構成について説明する。各装置は各々、装置全体を制御するCPU（Central Processing Unit）等の制御装置と、各種データや各種プログラムを記憶するROM（Read Only Memory）やRAM（Random Access Memory）等の記憶装置と、各種データや各種プログラムを記憶するHDD（Hard Disk Drive）やCD（Compact Disk）ドライブ装置等の外部記憶装置と、これらを接続するバスとを備えており、通常のコンピュータを利用したハードウェア構成となっている。また、各装置には各々、情報を表示する表示装置と、ユーザの指示入力を受け付けるキーボードやマウス等の入力装置と、外部装置の通信を制御する通信I/F（interface）とが有線又は無線により接続される。

[0016] 次に、上述したハードウェア構成において、配信開始ノードであるノード50のCPUが記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能について説明する。図2は、ノード50の機能的構成を例示する図である。ノード50は、固有情報格納部500と、乱数生成部501と、対称鍵生成部502と、ピース暗号化部503と、ピース化部504と、データ送信部505と、送信要求受付部506と、パラメータ生成部507と、変換部508とを有する。尚、固有情報格納部500は、例えばノード50のHDDなどの外部記憶装置に記憶領域として確保されるものである。乱数生成部501と、対称鍵生成部502と、ピース化部504と、ピース暗号化部503と、データ送信部505と、送信要求

受付部506と、パラメータ生成部507と、変換部508との実体は、ノード50のCPUのプログラム実行時にRAMなどの記憶装置上に生成されるものである。尚、ノード50の外部記憶装置には、配信データが予め記憶されている。

- [0017] 固有情報格納部500は、当該ノード50に割り当てられたノードID及び秘密鍵を記憶する。ピース化部504は、配信データを複数のピースに分割する。分割する際のデータサイズは特に限定されないが、予め定められているものとする。送信要求受付部506は、ピース化部504が分割したピースを要求するピース要求を他のノード51から受信する。乱数生成部501は、送信要求受付部506がピース要求を受信した場合、その発生毎に異なり得る一時情報である乱数を3つ生成する。一時情報とは、ノードで生成される度に異なり得る値となれば良く、乱数の他、例えば、タイムスタンプ、通信のシーケンス番号、ノードに固有のカウンタの値、Time Variant Parameterである。Time Variant Parameterについては、例えば文献ISO/IEC 9798-1に記載されている。ここで生成される乱数を r , r_0 , r'_0 とする。このうち、乱数 r , r_0 は、後述するように、ピースの暗号化に用いる対称鍵を毎回変化させるために用いられ、乱数 r'_0 は、変換を行う際に用いる変換パラメータを毎回変化させるために用いられる。

- [0018] 対称鍵生成部502は、乱数生成部501が生成した乱数のうち2つの乱数 r , r_0 と、固有情報格納部500に記憶された秘密鍵 s_0 とを用いて関数Fにより2つの対称鍵 k , k_0 を生成する。これを式により表すと以下のように表される。

$$k = F(s_0, r)$$

$$k_0 = F(s_0, r_0)$$

この関数Fは一方方向性関数であり、入力値である秘密鍵や乱数を知るものであってもこれらから出力値である対称鍵を推測できないものである。

- [0019] 尚、対称鍵がユーザにより不正に利用されることを防止するために、対称鍵生成部502は、生成した対称鍵を、ユーザに知られていない暗号鍵で更

に暗号化してHDDなどの外部記憶装置に記憶させ、対称鍵の実際の値をユーザに分からせないように秘匿することが望ましい。また、関数Fによる変換のアルゴリズムをユーザが特定できないように秘匿することが望ましい。

[0020] パラメータ生成部507は、乱数生成部501が生成した乱数のうち対称鍵の生成に用いられていない乱数 r'_0 と、秘密鍵 s_0 とを用いて関数Gにより変換パラメータ k'_0 を生成する。これを式により表すと以下のように表される。

$$k'_0 = G(s_0, r'_0)$$

この関数Gは一方方向性関数であり、出力値である変換パラメータと入力値である乱数を知るものであっても、これらから入力値である秘密鍵を推測できないものである。

[0021] 尚、変換パラメータがユーザにより不正に利用されることを防止するために、パラメータ生成部507は、生成した変換パラメータを、ユーザに知られていない暗号鍵で暗号化してHDDなどの外部記憶装置に記憶させ、変換パラメータの実際の値をユーザに分からせないように秘匿することが望ましい。

[0022] ピース暗号化部503は、対称鍵生成部502が生成した対称鍵のうち1つの対称鍵 k を用いてピースを暗号化して、暗号化ピースを出力する。尚、ピース P が対称鍵 k で暗号化された暗号化ピースを、 $E(k)P$ と表記する。また、ピース暗号化部503は、以下に説明する変換部508が暗号化ピース $E(k)P$ を変換したものを、対象鍵 k_0 を用いて更に暗号化して、新たな暗号化ピースを出力する。変換した暗号化ピースを $L(k'_0)E(k)P$ と表記すると、これを、対象鍵 k_0 を用いて暗号化した暗号化ピースを $E(k_0)L(k'_0)E(k)P$ と表記する。

[0023] 変換部508は、ピース暗号化部503が出力した暗号化ピース $E(k)P$ を、パラメータ生成部507が生成した変換パラメータ k'_0 を用いて関数Lにより変換する。変換した暗号化ピースを、 $L(k'_0)E(k)P$ と表記する。この関数Lによる変換は、各変換パラメータを1つの値に集約した変換パラメータ（集約パラメータ）を用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約パラメータを用いて逆変換が可

能である可逆な変換である。このような変換には例えば線形変換があるが、これに限るものではない。尚、関数 L による変換のアルゴリズムをユーザが特定できないように秘匿することが望ましい。関数 L 及び逆変換を行うための関数(関数 L^{-1} とする)の詳細については後述する。

[0024] データ送信部505は、ピース要求を送信した他のノード51に対して、固有情報格納部500に記憶されているノードIDと、乱数生成部501が生成した3つの乱数 r, r_0, r'_0 と、ピース暗号化部503が出力した新たな暗号化ピース $E(k_0)L(k'_0)E(k)P$ とを送信する。また、データ送信部505は、これらとは別に、対称鍵生成部502が生成した対称鍵のうち、変換された暗号化ピースの暗号化に用いられた対称鍵 k_0 を、ピース要求を送信した他のノード51に対して送信する。尚、対称鍵については、データ送信部505はSSL (Secure Socket Layer) などのプロトコルを利用して暗号化して送信することが望ましい。

[0025] 次に、配信開始ノード以外であるノード51のCPUが記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能について説明する。図3は、ノード51の機能的構成を例示する図である。ノード51は、固有情報格納部510と、乱数生成部511と、対称鍵生成部512と、ピース暗号化部513と、データ受信部514と、データ送信部515と、送信要求受付部516と、データ格納部517と、送信要求送信部518と、鍵要求送信部519と、ピース復号部520と、変換部521と、逆変換部522と、パラメータ生成部523とを有する。尚、固有情報格納部510とデータ格納部517とは、例えばノード51のHDDなどの外部記憶装置に記憶領域として確保されるものである。乱数生成部511と、対称鍵生成部512と、ピース暗号化部513と、データ送信部515と、送信要求受付部516と、データ受信部514と、鍵要求送信部519と、ピース復号部520と、変換部521と、逆変換部522と、パラメータ生成部523との実体は、ノード51のCPUのプログラム実行時にRAMなどの記憶装置上に生成されるものである。

[0026] 固有情報格納部 510 は、当該ノード 51 に割り当てられたノード ID 及び秘密鍵を記憶する。送信要求受付部 516 の構成は上述のノード 50 の有する送信要求受付部 506 の構成と同様である。送信要求送信部 518 は、ピースを要求するピース要求をノード 50 又は他のノード 51 に対して送信する。データ受信部 514 は、送信要求送信部 518 がピース要求を送信した相手であるノード 50 又は他のノード 51 から、変換され暗号化されたピースである暗号化ピースと、当該暗号化ピースの送信を仲介した少なくとも 1 つの他のノード 50, 51 に割り当てられた各ノード ID を含むノード ID 列と、当該他のノード 50, 51 が各々生成した乱数を含む乱数列とを受信する。また、データ受信部 514 は、これらとは別に、送信要求送信部 518 がピース要求を送信した相手であるノード 50 又は他のノード 51 が生成した対称鍵を受信する。データ格納部 517 は、データ受信部 514 が受信したノード ID 列、乱数列、暗号化ピース及び対称鍵を対応付けて記憶する。尚、受信した対称鍵を、上述したようにユーザに知られていない暗号鍵で更に暗号化して HDD などの外部記憶装置に記憶させるなどして秘匿することが望ましい。

[0027] 乱数生成部 511 は、一時情報である乱数を 2 つ生成する。1 つの乱数は、暗号化ピースの暗号化に用いる対称鍵を毎回変化させるために用いられ、もう 1 つの乱数は、変換を行う際に用いる変換パラメータを毎回変化させるために用いられる。

[0028] 対称鍵生成部 512 は、乱数生成部 511 が生成した乱数のうち 1 つの乱数と、固有情報格納部 510 に記憶された秘密鍵とを用いて上述した関数 F により対称鍵を生成する。ノード 51 においても対称鍵生成部 512 は、生成した対称鍵を上述したように秘匿することが望ましい。

[0029] パラメータ生成部 523 は、乱数生成部 511 が生成した乱数のうち対称鍵の生成に用いられていない乱数と、秘密鍵とを用いて上述の関数 G により変換パラメータを生成する。ノード 51 においてもパラメータ生成部 523 は、生成した変換パラメータを上述したように秘匿することが望ましい。

- [0030] ピース暗号化部 513 は、データ格納部 517 に暗号化ピースと対応付けられて記憶された対称鍵を用いて当該暗号化ピースを復号する。ここで復号された暗号化ピースを説明の便宜上、半復号ピースという。ピース暗号化部 513 は、以下に説明する変換部 521 が変換した半復号ピースを、対称鍵生成部 512 が生成した対称鍵を用いて暗号化して、新たな暗号化ピースを出力する。
- [0031] 変換部 521 は、ピース暗号化部 513 が復号して得た半復号ピースを、パラメータ生成部 523 が生成した変換パラメータを用いて上述の関数 L により変換する。
- [0032] データ送信部 515 は、ピース要求を送信した他のノード 51 に対して、固有情報格納部 510 に記憶されているノード ID と、乱数生成部 511 が生成した 2 つの乱数と、ピース暗号化部 513 が出力した新たな暗号化ピースとを送信する。また、データ送信部 515 は、これらとは別に、対称鍵生成部 512 が生成した対称鍵を、ピース要求を送信した他のノード 51 に対して送信する。
- [0033] ここで、ノード 50、51 から送信されるノード ID 列、乱数列、暗号化ピース及び対称鍵について具体的に説明する。尚、ノード 50 から 1 つの暗号化ピースに対してこれと共に送信されるノード ID は 1 つであるが、ここでは説明の便宜上、これらをノード列と記載する場合がある。暗号化ピースの配信経路としてここではノード 50 からノード 51A、更にノード 51A からノード 51B に暗号化ピースを送信し、ノード 51B から鍵サーバ 53 に鍵要求を送信する場合について説明する。例えば、あるピース P についてノード 51A からのピース要求に応じて、ノード 50 が、上述したように、乱数 r, r_0 と秘密鍵 s_0 とを用いて対称鍵 k, k_0 を各々生成し、対称鍵 k を用いてピース P を暗号化して暗号化ピース $E(k)P$ を出力する。そして、ノード 50 が、乱数 r'_0 と秘密鍵 s_0 とを用いて変換パラメータ k'_0 を生成し、変換パラメータ k'_0 を用いて暗号化ピース $E(k)P$ を変換し、変換した暗号化ピース $L(k'_0)E(k)P$ を、対称鍵 k_0 を用いて暗号化して新たな暗号化ピース $E(k_0)L(k'_0)E(k)P$ を出力する。そ

して、ノード50が、当該暗号化ピース $(k_0)L(k'_0)E(k)P$ をノードID#0及び乱数 r, r_0, r'_0 と共にノード51Aに送信し、これらとは別に対称鍵 k_0 をノード51Aに送信したとする。図4は、ノード50からノード51Aに送信される情報を模式的に示す図である。当該ノード51Aは、これらのノードID#0、乱数 r, r_0, r'_0 、暗号化ピース $E(k_0)L(k'_0)E(k)P$ 及び対称鍵 k_0 を対応付けてデータ格納部517に記憶することになる。尚、データ格納部517は、ノードIDと当該ノードIDが割り当てられたノードが生成した乱数との対応関係を保持した状態で各ノードID列及び各乱数列を記憶する。

[0034] そして、当該ノード51Aが、ノード51Bからのピース要求に応じてピースPに対する暗号化ピースを送信する場合、乱数 r_1, r'_1 を生成し、乱数 r_1 と秘密鍵 s_1 とを用いて対称鍵 k_1 を生成し、乱数 r'_1 と秘密鍵 s_{-1} とを用いて変換パラメータ k'_1 を生成する。また、ノード51Aが、データ格納部517に暗号化ピース $E(k_0)L(k'_0)E(k)P$ と対応付けられて記憶された対称鍵 k_0 を用いて当該暗号化ピースを復号する。この結果、半復号ピース $L(k'_0)E(k)P$ が得られる。そして、ノード51Aが、変換パラメータ k'_{-1} を用いて、半復号ピース $L(k'_0)E(k)P$ を変換する。この結果、変換された半復号ピース $L(k'_1)L(k'_0)E(k)P$ が得られる。そして、ノード51Aが、変換した半復号ピース $L(k'_1)L(k'_0)E(k)P$ を、自身が生成した対称鍵 k_1 を用いて暗号化して、新たな暗号化ピース $E(k_1)L(k'_1)L(k'_0)E(k)P$ を出力したとする。このとき、ノード51Aは、ノード51Bに対して、データ格納部517に記憶されている、ノード50に割り当てられたノードID#0に加え固有情報格納部510に記憶されている、自身に割り当てられたノードID#1と、データ格納部517に記憶されている乱数 r_0 に加え自身が生成した乱数 r_1, r'_1 と、新たな暗号化ピース $E(k_1)L(k'_1)L(k'_0)E(k)P$ とを送信する。また、ノード51Aは、これらとは別に、自身が生成した対称鍵 k_1 をノード51Bに対して送信する。図5は、ノード51Aからノード51Bに送信される情報を模式的に示す図である。ノード51Bは、これらのノードID列ID#0, ID#1、乱数列 r, r_0, r'_0, r_1, r'_1 、暗号化ピース $E(k_1)L(k'_1)L(k'_0)E(k)P$ 及び対称鍵 k_1 を対応付けてデータ格納部517に記憶する。

[0035] このように、暗号化ピースは、配信開始ノードであるノード50により最初に暗号化された状態で、当該暗号化ピースの送信を仲介した各ノード51によって変換が重ねて行われ、当該暗号化ピースを最後に送信したノード51によって最後に暗号化された状態となって、当該暗号化ピースを受信したノード51で記憶される。

[0036] 図3の説明に戻る。鍵要求送信部519は、データ格納部517に記憶された暗号化ピースを逆変換し復号するための復号情報を要求する鍵要求を鍵サーバ53に送信する。ここで鍵要求送信部519は、当該暗号化ピースに対応してデータ格納部517に記憶されているノードID列及び乱数列を鍵要求に含めて鍵サーバ53に送信する。例えば、ノード51Bが、図5に示した暗号化ピース $E(k_1)L(k'_1)L(k'_0)E(k)P$ に対する鍵要求を鍵サーバ53に送信する場合、ノード51Bの鍵要求送信部519は、ノードID列ID#0, ID#1と、乱数列 r, r_0, r'_0, r_1, r'_1 とを含む鍵要求を送信する。図6は、ノード51Bから鍵サーバ53に送信される情報を模式的に示す図である。このように、ノード51は、暗号化ピースを逆変換し復号するための復号情報を鍵サーバ53に要求する際に、当該暗号化ピースの配信経路を示すものとして、配信開始ノードであるノード50を基点として当該暗号化ピースの送信を仲介した各ノード50, 51の各ノードIDを含むノードID列及び当該各ノード50, 51が生成した乱数を含む乱数列を鍵サーバ53に送信する。尚、これらの送信に際し、鍵要求送信部519は、各ノードIDと当該各ノードIDが割り当てられたノードが出力した乱数との対応関係を保持した状態で送信する。

[0037] ピース復号部520は、鍵要求送信部519が送信した鍵要求に応じて鍵サーバ53から送信された2つの対称鍵と変換パラメータとを含む復号情報を受信する。尚、2つの対称鍵とは、配信開始ノードであるノード50が生成した対称鍵のうちピースの暗号化に最初に用いた対称鍵と、当該ノード51に対して暗号化ピースを最後に送信したノード51（最終ノードという）が生成して暗号化に用いた対称鍵とである。また、ここで受信する変換パラ

メータは、当該暗号化ピースの送信を仲介した各ノードが生成した各変換パラメータを1つの値に集約した変換パラメータ（集約パラメータという）である。集約パラメータの詳細については後述する。図7は、鍵サーバ53からノード51Bに送信される復号情報を模式的に示す図である。同図に示されるように、ノード51Bは、図6に示したノードID列及び乱数列を含む鍵要求に応じて鍵サーバ53から送信された対称鍵 k, k_1 と、集約パラメータ k'_1 とを含む復号情報を受信する。

[0038] そして、ピース復号部520は、まず、受信した対称鍵のうち、最終ノードが生成した対称鍵を用いて、暗号化ピースを復号する。この結果半復号ピースが得られる。次いで、ピース復号部520は、得られた半復号ピースに対して、集約パラメータを用いて関数 L^{-1} により逆変換を逆変換部522に行わせ、逆変換を行った半復号ピースを、受信した対称鍵のうち配信開始ノードであるノード50が生成した対称鍵を用いて復号する。この結果、利用可能なピースが得られる。

[0039] 逆変換部522は、ピース復号部520の制御の下、ピース復号部520が得た半復号ピースに対して、集約パラメータを用いて関数 L^{-1} により逆変換を行う。

[0040] 尚、ノード51が、複数のピースのそれぞれについてどのような順番やタイミングでどのノードから取得するかは特に限定されないが、以上のようにして、ノード51は、複数のピースのそれぞれが暗号化された各暗号化ピースをピース要求によって他のノード50、51から取得する。また、ノード51は、各暗号化ピースについて鍵要求によって各対称鍵及び集約パラメータを含む復号情報を鍵サーバ53から受信し、各暗号化ピースを復号することにより、上述の配信データを得る。

[0041] 次に、鍵サーバ53のCPUが記憶装置や外部記憶装置に記憶された各種プログラムを実行することにより実現される各種機能について説明する。図8は、鍵サーバ53の機能的構成を例示する図である。鍵サーバ53は、秘密鍵格納部530と、データ受信部531と、パラメータ生成部532と、

対称鍵生成部533と、データ送信部534とを有する。尚、秘密鍵格納部530は、例えば鍵サーバ53のHDDなどの外部記憶装置に記憶領域として確保されるものである。データ受信部531と、パラメータ生成部532と、対称鍵生成部533と、データ送信部534との実体は、鍵サーバ53のCPUのプログラム実行時にRAMなどの記憶装置上に生成されるものである。

[0042] 秘密鍵格納部530は、各ノード50、51に割り当てられた秘密鍵を、各ノード50、51に割り当てられたノードIDと対応付けて記憶する。データ受信部531は、暗号化ピースを逆変換し復号するための復号情報を要求すると共に上述したノードID列及び乱数列を含む鍵要求をノード51から受信する。

[0043] パラメータ生成部532は、データ受信部531が受信した鍵要求に含まれるノードID列のうち、ピースを最初に暗号化した配信開始ノードであるノード50及び鍵要求を送信したノード51に対して暗号化ピースを最後に暗号化して送信したノード51（最終ノード）に各々対応付けられて秘密鍵格納部530に記憶されている秘密鍵を読み出しこれと、当該鍵要求に含まれる乱数列に含まれる、ノード50が生成した乱数のうちピースに対する最初の暗号化に用いた対称鍵の生成に用いた乱数及び最終ノードが生成した乱数のうち対称鍵の生成に用いた乱数を用いて関数Fにより2つの対称鍵を生成する。例えば、鍵要求を送信したノード51のノードIDがID#(j)であり、鍵要求に含まれるノードID列に含まれる各ノードIDがID#0, ..., ID#(j-1)であり、各ノードID ID#m ($0 \leq m \leq j$) に r_m, s_m が各々対応しているものとする。配信開始ノードであるノード50の秘密鍵は s_0 であり、最終ノードの秘密鍵は s_{j-1} である。また、ノード50が生成した乱数のうち対称鍵の生成に用いた乱数の1つは、 r である。最終ノードが生成した乱数のうち対称鍵の生成に用いた乱数は、 r_{j-1} である。この場合、対称鍵生成部533は、以下の式により表される2つの対称鍵 k, k_{j-1} を生成する。この結果、ピースに対する最初の暗号化に用いられた対称鍵 k と、最後の暗号化に用いられた対称鍵 k_{j-1} との2つが

得られる。

$$k = F(s_0, r)$$

$$k_{j-1} = F(s_{j-1}, r_{j-1})$$

- [0044] また、パラメータ生成部 532 は、データ受信部 531 が受信した鍵要求に含まれるノード ID 列に含まれる各ノード ID に対応付けられている秘密鍵と、鍵要求に含まれる、各ノード ID に対応する乱数列とを用いて、上述の関数 G により変換パラメータをノード ID 毎に各々生成する。各 m ($0 \leq m \leq j$) についての変換パラメータは以下の式により表される。

$$k'_m = G(s_m, r'_m)$$

- [0045] そして、パラメータ生成部 532 は、生成した全ての変換パラメータを用いて、関数 H によりこれらの変換パラメータを 1 つの値に集約する。このようにしてパラメータ生成部 532 は集約パラメータを生成する。尚、関数 H は、集約パラメータを用いて変換を行った結果と、各変換パラメータを用いて各変換を重ねて行った結果とが同一となるような変換において、複数の変換パラメータを 1 つの変換パラメータ（集約パラメータ）に集約するための関数である。即ち、 k_1, k_2 を任意のパラメータとすると、関数 L 及び関数 H については以下の式が成り立つ。

$$L(k_2) L(k_1) = L(H(k_1, k_2))$$

- [0046] ここで、本実施の形態にかかる集約パラメータを k'_{*j-1} とすると、 k'_{*j-1} は以下の式により表される。

$$k'_{*j-1} = H(k'_0, k'_1, \dots, k'_{j-1})$$

- [0047] データ送信部 534 は、対称鍵生成部 533 が生成した対称鍵及びパラメータ生成部 532 が生成した集約パラメータとを含む復号情報を、データ受信部 531 が受信した鍵要求を送信したノード 51 に対して送信する。

- [0048] 例えば、鍵サーバ 53 は、図 6 に示されるノード ID 列及び乱数列を含む鍵要求に応じて、乱数 r, r_1 から各々対称鍵 k, k_1 を得て、変換パラメータ k'_0, k'_1 を集約した変換パラメータを k'_* を得て、図 7 に示されるように、これらを含む復号情報をノード 51 B に対して送信する。

[0049] ここで、関数 L , L^{-1} について説明する。関数 L については、例えば、以下の (a-1) ~ (a-4) に示される各関数が考えられる。

(a-1) 排他的論理和

$$L(k)P = P + k$$

$$L(k_1)L(k_2) = L(k_1 + k_2)$$

$$H(k_1, k_2) = k_1 + k_2$$

(a-2) 有限体上の乗算

$$k = k(1) | k(2) | \dots | k(m)$$

$$P = P(1) | P(2) | \dots | P(m)$$

k, P は m 個の n ビットの要素に等分されるとする。ここで、 $|$ は接続を表す。

各 $k(i), P(i)$ を有限体 $GF(2^n)$ 上の要素とみなし、乗算を $*$ で表す。

$k(i)$ は逆元を持つと仮定する。

$$L(k)P = k(1) * P(1) | k(2) * P(2) | \dots | k(m) * P(m)$$

$$L(k_2)L(k_1)P = k_1(1) * k_2(1) * P(1) | k_1(2) * k_2(2) * P(2) | \dots | k_1(m) * k_2(m) * P(m)$$

$$H(k_1, k_2) = k_1(1) * k_2(1) | k_1(2) * k_2(2) | \dots | k_1(m) * k_2(m)$$

$$H(k_1, k_2, k_3) = k_1(1) * k_2(1) * k_3(1) | k_1(2) * k_2(2) * k_3(2) | \dots | k_1(m) * k_2(m) * k_3(m)$$

(a-3) 剰余加算

$$k = k(1) | k(2) | \dots | k(m)$$

$$P = P(1) | P(2) | \dots | P(m)$$

各 $k(i), P(i)$ を剰余類 $2^n\mathbb{Z}/\mathbb{Z}$ ($\mathbb{Z}_2^n$ と書く) の要素とみなし、加算を $+$ で表す。

(注：正式には、 $P(i) + k(i) \bmod(2^n)$ などと書く。)

$$L(k)P = k(1) + P(1) | k(2) + P(2) | \dots | k(m) + P(m)$$

$$L(k_2)L(k_1) = k_1(1) + k_2(1) | k_1(2) + k_2(2) | \dots | k_1(m) + k_2(m)$$

$$H(k_1, k_2) = k_1(1) + k_2(1) | k_1(2) + k_2(2) | \dots | k_1(m) + k_2(m)$$

$$H(k_1, k_2, k_3) = k_1(1) + k_2(1) + k_3(1) | k_1(2) + k_2(2) + k_3(2) | \dots | k_1(m) + k_2(m) + k_3(m)$$

(a-4) 有限体上の乗算と加算の組合せ

$$L(k, q)P = k(1) * P(1) + q(1) | k(2) * P(2) + q(2) | \dots | k(m) * P(m) + q(m)$$

$$L(k_2, q_2)L(k_1, q_1)P = k_2(1) * [k_1(1) * P(1) + q_1(1)] + q_2(1) | \dots$$

$$=k_1(1)*k_2(1)*P(1)+[k_2(1)*q_1(1)+q_2(1)]|\dots$$

$$L(k_2, q_2) L(k_1, q_1) = L(k_1 * k_2, k_2 * q_1 + q_2)$$

$$H(k_1, q_1, k_2, q_2) = (k_1 * k_2, k_2 * q_1 + q_2)$$

[0050] また、関数 L^{-1} については、例えば、以下の (b-1) ~ (b-4) に示す各条件を満たす関数が考えられる。

(b-1) 排他的論理和

$$L^{-1}(k) = L(k)$$

即ち、関数 L と関数 L^{-1} とは同一の関数である。

この場合、

$$L^{-1}(k) L(k) P = L(k) L(k) P = L(k) (P+k) = (P+k) + k = P+k+k = P+0 = P$$

(b-2) 有限体上の乗算

$$k = k(1) | k(2) | \dots | k(m)$$

$$P = P(1) | P(2) | \dots | P(m)$$

$$k(i) \text{ の逆元を } k(i)^{-1} \text{ とする。つまり、} k(i)^{-1} * k(i) = k(i) * k(i)^{-1} = 1$$

ここで、 k^{-1} を次のように定義する。

$$k^{-1} = k(1)^{-1} | k(2)^{-1} | \dots | k(m)^{-1}$$

このとき、

$$L^{-1}(k) = L(k^{-1})$$

即ち、

$$L^{-1}(k) L(k) P = L(k^{-1}) [k(1) * P(1) | k(2) * P(2) | \dots | k(m) * P(m)]$$

$$= k(1)^{-1} * k(1) * P(1) | k(2)^{-1} * k(2) * P(2) | \dots | k(m)^{-1} * k(m) * P(m)$$

$$= P(1) | P(2) | \dots | P(m)$$

(b-3) 剰余加算

$$k = k(1) | k(2) | \dots | k(m)$$

$$P = P(1) | P(2) | \dots | P(m)$$

$$L^{-1}(k) = L(2^n - k)$$

(注: $L(-k)$ としても良いが、値を $0 \sim 2^n - 1$ の範囲にするために 2^n を足した。)

即ち、

$$\begin{aligned}
L^{-1}(k) L(k) P &= L(2^n - k) [P(1) + k(1) | P(2) + k(2) | \cdots | P(m) + k(m)] \\
&= P(1) + k(1) + 2^{n-k(1)} | P(2) + k(2) + 2^{n-k(2)} | \cdots | P(m) + k(m) + 2^{n-k(m)} \\
&= P(1) + 2^n | P(2) + 2^n | \cdots | P(m) + 2^n \\
&= P(1) | P(2) | \cdots | P(m)
\end{aligned}$$

(b-4) 有限体上の乗算と加算の組合せ

$$\begin{aligned}
L(k, q) P &= k(1) * P(1) + q(1) | k(2) * P(2) + q(2) | \cdots | k(m) * P(m) + q(m) \\
L^{-1}(k, q) &= L(k^{-1}, 2^n - k^{-1} * q)
\end{aligned}$$

即ち、

$$\begin{aligned}
L^{-1}(k, q) L(k, q) P &= L(k^{-1}, 2^n - k^{-1} * q) [k(1) * P(1) + q(1) | \cdots] \\
&= k(1)^{-1} [k(1) * P(1) + q(1)] + (2^n - k(1)^{-1} * q(1)) | \cdots \\
&= P(1) + k(1)^{-1} * q(1) + 2^n - k(1)^{-1} * q(1) | \cdots \\
&= P(1) + 2^n | \cdots \\
&= P(1) | \cdots = P
\end{aligned}$$

[0051] 次に、本実施の形態にかかるデータ配信システムで行われる処理の手順について説明する。まず、配信開始ノードであるノード50が行う配信処理の手順について図9を用いて説明する。ノード50は、配信データを複数のピースに分割する（ステップS1）。そして、ノード50は、ピースを要求するピース要求を他のノード51から受信すると（ステップS2：YES）、乱数 r, r_0, r'_0 を生成する（ステップS3）。次いで、ノード50は、ステップS3で生成した乱数 r, r_0 と固有情報格納部500に記憶された秘密鍵 s_0 とを用いて関数Fにより対称鍵 k, k_0 を生成する（ステップS4）。次いで、ノード50は、ステップS3で生成した乱数 r'_0 と秘密鍵 s_0 とを用いて関数Gにより変換パラメータ k'_0 を生成する（ステップS5）。そして、ノード50は、ステップS4で生成した対称鍵 k を用いて、送信対象となるピースPを暗号化する（ステップS6）。尚、送信対象となるピースをどのように決定するかは特に限定されない。次いで、ノード50は、暗号化したピース（暗号化ピース） $E(k)P$ に対して、ステップS5で生成した変換パラメータ k'_0 を用いて関数Lにより暗号化ピース $E(k)P$ を変換する（ステップS7）。その後、ノード50

は、ステップS 7で変換した暗号化ピース $L(k'_0)E(k)P$ を、対称鍵 k_0 を用いて暗号化して新たな暗号化ピース $E(k_0)L(k'_0)E(k)P$ を出力する（ステップS 8）。そして、ノード5 0は、ステップS 2で受信されたピース要求を送信した他のノード5 1に対して、例えば図4に示されるように、固有情報格納部5 0 0に記憶されているノードID#0と、ステップS 3で生成した乱数 r, r_0, r'_0 と、ステップS 8で出力した暗号化ピース $E(k_0)L(k'_0)E(k)P$ とを送信する（ステップS 9）。また、ノード5 0は、これらとは別に、ステップS 4で生成した対称鍵 k_0 を当該他のノード5 1に対して送信する（ステップS 10）。その後ステップS 2に戻り、ノード5 0は、新たなピース要求の受信を待機する。尚、ステップS 2で受信されるピース要求は、同一のノード5 1であるとは限らず、当該ピース要求によって要求されるピースPは、同一のピースであるとは限らない。また、ステップS 3で生成する乱数は基本的にステップS 3の処理毎に異なる。

[0052] 次に、ノード5 1がノード5 0又は他のノード5 1から暗号化ピースを受信する受信処理の手順について図10を用いて説明する。ノード5 1は、ピースを要求するピース要求をノード5 0又は他のノード5 1に対して送信する（ステップS 20）。次いで、ノード5 1は、ステップS 20でピース要求を送信した相手であるノード5 0又は他のノード5 1から、ノードID列と、乱数列と、暗号化ピースとを受信し（ステップS 21）、これらとは別に対称鍵を受信する（ステップS 22）。そして、ノード5 1は、ステップS 21で受信したノードID列、乱数列及び暗号化ピースと、ステップS 22で受信した対称鍵とを対応付けて記憶する（ステップS 23）。

[0053] 尚、ノード5 1がノード5 0にピース要求を送信した場合は、ステップS 21ではピースPについて図4に示されるノードID列と、乱数列と、暗号化ピースとを受信する。ここで、図示はしないが、P2PネットワークNTに接続されるノードであって、 f を1以上の整数として、 f 番目にピースPを受信するノードについて一般化して説明する。説明の便宜上、当該ノードのノードIDをID# f とする。ノードID# f が割り当てられたノードは、 $(f-1)$ 番目

のノード $ID\#(f-1)$ が割り当てられたノードから、図 11 に示されるように、ピース P について、ノード ID 列 $ID\#0, \dots, ID\#(f-1)$ と、乱数 $r, r_0, r'_0, \dots, r'_{f-1}, r_{f-1}$ と、暗号化ピース $E(k_{f-1})L(k'_{f-1}) \cdots L(k'_0)E(k)P$ とを受信する。

[0054] 次に、配信開始ノード以外のノード 51 が行う配信処理の手順について図 12 を用いて説明する。ノード 51 は、ピースを要求するピース要求を他のノード 51 から受信すると（ステップ S30 : YES）、乱数を 2 つ生成する（ステップ S31）。次いでノード 51 は、ステップ S31 で生成した乱数のうち 1 つと、固有情報格納部 510 に記憶された秘密鍵とを用いて関数 F により対称鍵を生成する（ステップ S32）。次いで、ノード 51 は、ステップ S31 で生成した乱数のうち対称鍵の生成に用いていない乱数と、秘密鍵とを用いて上述の関数 G により変換パラメータを生成する（ステップ S33）。また、ノード 51 は、データ格納部 517 に暗号化ピースと対応付けられて記憶された対称鍵を用いて当該暗号化ピースを復号する（ステップ S34）。この結果半復号ピースが得られる。その後、ノード 51 は、ステップ S34 で得た半復号ピースを、ステップ S33 で生成した変換パラメータを用いて変換する（ステップ S35）。そして、ノード 51 は、ステップ S35 で変換した半復号ピースを、ステップ S32 で生成した対称鍵を用いて暗号化して、新たな暗号化ピースを出力する（ステップ S36）。その後ノード 51 は、ステップ S30 で受信されたピース要求を送信した他のノード 51 に対して、送信対象である暗号化ピースに対応付けられてデータ格納部 517 に記憶されたノード ID に加え固有情報格納部 510 に記憶されたノード ID を含む新たなノード ID 列と、当該暗号化ピースに対応付けられてデータ格納部 517 に記憶された乱数列に加えステップ S31 で生成した乱数を含む新たな乱数列と、ステップ S36 で出力した新たな暗号化ピースとを送信する（ステップ S37）。また、ノード 51 は、これらとは別に、ステップ S32 で生成した対称鍵を当該他のノード 51 に対して送信する（ステップ S38）。

[0055] 例えば、上述したノード $ID\#f$ が割り当てられたノードは、ステップ S

36では、 $(f+1)$ 番目となるノード $IDID\#(f+1)$ が割り当てられたノードに対して、図13に示されるように、ピースPについて、ノードID列 $ID\#0, \dots, ID\#(f-1), ID\#f$ と、乱数列 $r, r_0, r'_0, \dots, r_{f-1}, r'_{f-1}, r_f, r'_f$ と、暗号化ピース $E(k_f)L(k'_f)L(k'_{f-1}) \dots L(k'_0)E(k)P$ とを送信する。

[0056] 次に、ノード51が鍵サーバ53から復号鍵を取得しこれを用いて暗号化ピースを復号する復号処理の手順について図14を用いて説明する。ノード51は、データ格納部517に記憶された暗号化ピースに対応付けられているノードID列及び乱数列を読み出し（ステップS40）、当該暗号化ピースを逆変換し復号するための復号情報を要求すると共に、当該ノードID列及び乱数列を含む鍵要求を鍵サーバ53に送信する（ステップS41）。次いで、ノード51は、ステップS40で送信された鍵要求に応じて鍵サーバ53から送信された2つの対称鍵及び集約パラメータを含む復号情報を受信する（ステップS42）。2つの対称鍵とは、上述したように、ノード50が生成した対称鍵のうちピースの暗号化に最初に用いられた対称鍵と、最終ノードが生成した対称鍵であり最後の暗号化に用いられた対称鍵とである。ノード51は、まず、受信した対称鍵のうち、最終ノードが生成した対称鍵を用いて、暗号化ピースを復号する（ステップS43）。この結果半復号ピースが得られる。次いで、ノード51は、ステップS43で得た半復号ピースに対して、ステップS42で受信した集約パラメータを用いて関数 L^{-1} により逆変換を行う（ステップS44）。その後、ノード51は、ステップS44で逆変換を行った半復号ピースを、ステップS43で受信した対称鍵のうち、ノード50が生成した対称鍵を用いて復号する（ステップS45）。この結果、利用可能なピースが得られる。

[0057] 例えば、上述したノード $IDID\#(f+1)$ が割り当てられたノードは、鍵サーバ53に対して、図15に示されるように、ピースPについて、ノードID列 $ID\#0, \dots, ID\#(f-1), ID\#f$ と、乱数列 $r, r_0, r'_0, \dots, r_{f-1}, r'_{f-1}, r_f, r'_f$ とを送信する。そして、当該ノードは、鍵サーバ53から、図16に示されるように、ピースPについて、対称鍵 $k, \dots, k_{f-1}$ 及び集約パラメータ $[k'_{*f-1} = H(k'_{f-1}, \dots, k'_0)]$

」を含む復号情報を受信し、これを用いて暗号化ピース $E(k_f)L(k'_f)L(k'_{f-1})\cdots L(k'_0)E(k)P$ を復号して、ピース P を得る。このようにして、各ノード51は、複数のピースのそれぞれが暗号化された各暗号化ピースについて鍵要求によって各対称鍵及び集約パラメータを含む復号情報を鍵サーバ53から受信し、各暗号化ピースを復号することにより、上述の配信データを得ることができる。

[0058] 次に、鍵サーバ53がノード51からの鍵要求に応じて復号情報を送信する復号情報送信処理の手順について図17を用いて説明する。鍵サーバ53は、暗号化ピースを逆変換し復号するための復号情報を要求すると共に、ノードID列及び乱数列を含む鍵要求をノード51から受信すると（ステップS50：YES）、受信した鍵要求に含まれるノードID列に含まれる各ノードIDに対応付けられて秘密鍵格納部530に記憶されている秘密鍵をノードID毎に読み出す（ステップS51）。そして、鍵サーバ53は、配信開始ノードであるノード50が生成した乱数のうち最初の暗号化に用いた対称鍵の生成に用いた乱数及び最終ノードが生成した乱数のうち対称鍵の生成に用いた乱数を用いて関数Fにより2つの対称鍵を生成する（ステップS52）。2つの対称鍵とは、上述したように、ノード50が生成した対称鍵のうちピースの暗号化に最初に用いられた対称鍵と、最終ノードが生成した対称鍵であり最後の暗号化に用いられた対称鍵とである。そして鍵サーバ53は、ノードID列に含まれる各ノードIDに対応付けられている秘密鍵と、鍵要求に含まれる、各ノードIDに対応する乱数列とを用いて、上述の関数Gにより変換パラメータをノードID毎に各々生成する（ステップS53）。次いで、鍵サーバ53は、ステップS53で生成した全ての変換パラメータを用いて、関数Hによりこれらの変換パラメータを1つの値に集約して、集約パラメータを生成する（ステップS54）。その後、鍵サーバ53は、ステップS52で生成した対称鍵及びステップS54で生成した集約パラメータを含む復号情報を、ステップS50で受信した鍵要求を送信したノード51に対して送信する（ステップS55）。

[0059] 例えば、鍵サーバ53は、上述したノードID#(f+1)が割り当てられたノードに対して、ピースPについて、図15に示されるようなノードID列及び乱数列を含む鍵要求に応じて、図16に示されるような対称鍵 k, k_{f-1} 及び集約パラメータ $H(k'_{f-1}, \dots, k'_0)$ を送信する。

[0060] 以上のような構成によって、各ノード50, 51がピースを送信する度に、当該ピースに基本的に一度限りの対称鍵を用いて暗号化を行うが、暗号化を単純に重ねるのではなく、ピースに対する最後の暗号化に用いられた対称鍵を用いて、暗号化を一旦解いてから、一時的に生成した変換パラメータを用いて変換を行い、新たに生成した対称鍵を用いて暗号化を行う。即ち、あるノード51が取得した暗号化ピースは、配信開始ノードが最初に行った暗号化と、当該暗号化ピースの送信を仲介したノード51が各々重ねて行った変換と、当該ノードに当該暗号化ピースを最後に暗号化して送信した最後ノードが行った暗号化とが行われた状態となる。暗号化ピースが送信される過程で各ノード50, 51により各々重ねて行われる変換のシーケンスは、配信経路に応じて様々なものとなる。また、複数のピースのそれぞれが暗号化された全ての暗号化ピースの組み合わせについてみれば、暗号化ピースが異なれば配信経路が各々異なる可能性が高いため、各暗号化ピースにおいて行われている変換のシーケンスも各々異なっている可能性が高い。また、異なる暗号化ピースの配信経路が同じ場合、各暗号化ピースに対応付けられるノードIDの組み合わせは同じになるが、各ノードで暗号化に用いる対称鍵はその都度異なり得る。このため、配信経路が仮に同一であっても、暗号化を解くための対称鍵は各々異なり得る。以上のように、ノード毎及びピース毎に配信経路は異なり得るため、あるノードが取得する暗号化ピースの組み合わせは配信経路と配信時期とに固有のものとなり、確実に一意となり得る。また、いずれのノード51であっても、ピースに対する最初の暗号化及び最後の暗号化を解くための復号2回と、集約パラメータを用いた逆変換1回との計算で暗号化ピースを利用可能な状態に復号することができ、復号及び逆変換にかかる計算量を一定にすることができる。従って、ノード51の処理

負担を軽減させることができる。また、暗号化に用いる対称鍵を、乱数を用いて生成することで基本的に一度限りのものとするため、対称鍵の漏洩による影響を低減することができる。

[0061] 従って、以上のような構成によれば、P2P配信において配信方法に関する特別な工夫をしなくても、各ノードが取得する各暗号化ピースの組み合わせについてノード毎の一意性を確実に高めることができ、安全性を向上させることができる。更に、データの保護とデータの配信方法との独立性を維持することが可能になり、システム構築上の自由度を向上させることが可能になり、更に、通信装置における計算の効率を向上可能になる。

[0062] [変形例]

なお、本発明は前記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、前記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。また、以下に例示するような種々の変形が可能である。

[0063] 上述した実施の形態において、各ノード50で実行される各種プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成しても良い。また当該プログラムを、インストール可能な形式又は実行可能な形式のファイルでCD-ROM、フレキシブルディスク（FD）、CD-R、DVD（Digital Versatile Disk）等のコンピュータで読み取り可能な記録媒体に記録して提供するように構成しても良い。この場合には、プログラムは、各ノード50において上記記録媒体から読み出して実行することにより主記憶装置（例えばRAM）上にロードされ、上記機能的構成において説明した各部が主記憶装置上に生成される。鍵サーバ53で実行される各種プログラムについても同様である。

- [0064] また、上述した実施の形態において、各ノード50の機能的構成において説明した各部のうち全部又は一部をハードウェアにより構成しても良い。鍵サーバ53の機能的構成において説明した各部のうち全部又は一部についても同様である。
- [0065] 上述した実施の形態において、ノードIDは、各ノードを一意に識別可能な情報であれば良く、例えば、各ノードのIPアドレスや、MACアドレスや、URLなどであっても良い。
- [0066] 上述した実施の形態のデータ配信システムにおいては、配信開始ノードの数は複数であっても良い。また、P2PネットワークNTに接続されるこの他のノードの数も特に限定されない。
- [0067] 上述の実施の形態においては、1つのピース要求によって複数のピースが要求されるようにしても良い。この場合、ノード50、51は、複数のピースのそれぞれについて上述したように暗号化ピース、ノードID列及び乱数列の組を、ピース要求を送信した他のノード51に送信すれば良い。
- [0068] また、上述の実施の形態においては、ノード50、51は、ピース要求に応じて暗号化ピースを送信する構成としたが、これに限らず、ピース要求を受信しなくとも、他のノード51に暗号化ピースと共にIDノード列及び乱数列を送信するようにしても良い。
- [0069] 上述の実施の形態においては、ノード51は、配布データを構成する全てのピースについて暗号化ピースが取得されデータ格納部517に記憶された場合に、各暗号化ピースを逆変換し復号するための各復号情報を要求する鍵要求を鍵サーバ53に送信するようにしても良い。又は、ノード51は、配布データを構成する全てのピースについて暗号化ピースが取得されていない場合であっても、データ格納部517に記憶された暗号化ピースに対する鍵要求を鍵サーバ53に送信するようにしても良い。また、ノード51は、1つの鍵要求によって、1つの暗号化ピースを逆変換し復号するための復号情報を要求するようにしても良いし、複数の暗号化ピースを各々逆変換し復号するための各復号情報を要求するようにしても良い。

- [0070] 上述の実施の形態においては、ピースの暗号化には、暗号鍵でもあり、暗号化を復号するための復号鍵でもある対称鍵を用いた。しかし、ピースの暗号化に用いる暗号鍵と、暗号化ピースに対して行われている暗号化を復号するための復号鍵とは各々別であるとしても良い。
- [0071] また、上述の実施の形態においては、ノード50, 51は、データ格納部517に記憶された暗号化ピースを他のノード51に送信する場合、その都度、乱数を生成するようにした。しかし、ノード50, 51は、乱数をその都度生成するのではなく、例えば、暗号化ピースの送信回数に応じて発生させるようにしても良い。例えば、ノード50, 51は、暗号化ピースの送信を所定の回数（例えば5回）行う毎に新たな乱数を生成するようにしても良い。また、ノード50, 51が乱数を生成するタイミングは、他のノード51からピース要求を受信したときであっても良いし、所定の時間毎であっても良い。
- [0072] また、上述の実施の形態においては、ノード51は、データ格納部517に記憶された暗号化ピースを暗号化して他のノード51に送信する場合、当該暗号化ピースのデータの全部ではなく一部のデータについて暗号化するようにしても良い。この場合、当該暗号化ピースの配信を仲介する各ノード51が暗号化するデータが、同じく当該暗号化ピースの配信を仲介する他のノード51が暗号化するデータと重複部分が生じるように、各ノード51は当該暗号化ピースの一部のデータを暗号化するようにすれば良い。このような構成によれば、各ノード51が行う暗号化に関する処理負担を軽減させることができると共に、暗号化部分を重複させることにより、復号鍵が暴露された場合の影響を抑制することが可能になる。
- [0073] 上述の実施の形態においては、ノード51が他のノード51に暗号化ピースと共に送信するノードID列及び乱数列は、図5, 11, 13に示される形態に限らない。例えば、 $(ID\#0, r_0), (ID\#1, r_1) \cdots (ID\#f, r_f)$ などのように、ノードIDと当該ノードIDに対応する乱数との組をノードID毎に示す形態であっても良い。

- [0074] 上述の実施の形態においては、各ノード50, 51に一意に割り当てられた秘密鍵として秘密鍵を用いたが、これに限らない。
- [0075] また、上述の実施の形態においては、秘密鍵は、各ノード50, 51に一意に割り当てられているとしたが、これに限らない。例えば、各ノード50, 51のうち一部のノードに同一の秘密鍵が割り当てられるようにしても良い。
- [0076] 上述の実施の形態においては、上述した暗号化ピース、ノードID列及び乱数列をパッケージ化したパッケージデータの形態で配布されるように構成しても良い。この場合、パッケージデータはコンピュータで読み取り可能な記録媒体に記録されてノードに提供されるようにしても良いし、サーバを介してノードにダウンロードされるように構成しても良い。当該パッケージデータを取得したノードは、ピース要求に応じて、上述の実施の形態と同様に、当該パッケージデータに含まれる暗号化ピースに対して暗号化を選択的に行った暗号化ピースと、パッケージデータに含まれるノードID及び自身のノードIDと、パッケージデータに含まれる乱数列及び自身が生成した乱数とを他のノードに送信すれば良い。
- [0077] 上述した実施の形態においては、ID列、乱数列及び暗号化ピースの送信と、対称鍵の送信とを分けるようにしたが、ノード50, 51は、これらを同時に送信するようにしても良い。
- [0078] 上述した実施の形態においては、変換パラメータの生成に用いる乱数と、対称鍵の生成に用いる乱数とを異なるようにした。しかし、ノード50, 51は、変換パラメータ及び対称鍵を同一の乱数を用いて生成しても良い。
- [0079] 上述した実施の形態においては、鍵サーバ53は、集約パラメータと、ピースに対する最初の暗号化に用いられた対称鍵と、最後の暗号化に用いられた対称鍵とを含む復号情報をノード51に送信するようにした。しかし、鍵サーバ53は、最後の暗号化に用いられた対称鍵を含まず、集約パラメータと、ピースに対する最初の暗号化に用いられた対称鍵とを含む復号情報をノード51に送信するようにしても良い。
- [0080] 上述の実施の形態においては、コンテンツを構成する各ピースに対しては

、1回又は2回の暗号化が行われている状態にしたが、3回以上の暗号化が多重に行われている状態にするコンテンツ配信システムに本実施の形態を適用にするようにしても良い。

[0081] ここでまず、ピースを複数の暗号鍵で3回以上多重に暗号化するコンテンツ配信システムについて説明する。各ノード50, 51には、上述の実施の形態と同様に秘密鍵及びノードIDが各々割り当てられており、ノード50, 51は、例えば、自身に割り当てられた秘密鍵を暗号鍵として用いて、自身が分割したピース又は他のノード50, 51から受信した暗号化ピースを暗号化して、暗号化したものをその他のノード51に送信する。このように、暗号化ピースが各ノード50, 51から送信される度に暗号化が施されるようにする。具体的には、例えば、配信開始ノードであるノード50は、他のノード51からピース要求を受信すると、秘密鍵を用いてピースを暗号化した後、暗号化ピースと自身に割り当てられたノードIDとを当該他のノード51に送信する。ノード51は、暗号化ピース及びノードIDを対応付けて記憶する。そして、ノード51は、他のノード51からピース要求を受信すると、自身に割り当てられた秘密鍵を用いて暗号化ピースを更に暗号化して新たな暗号化ピースを出力し、当該暗号化ピースと対応付けて記憶したノードID及び自身に割り当てられたノードIDと新たな暗号化ピースを他のノード51に送信する。他のノード51においても同様にピース要求を受信した場合には、送信対象の暗号化ピースに対して更なる暗号化を行って、当該暗号化ピースと対応付けて記憶したノードID及び自身に割り当てられたノードIDと新たな暗号化ピースとを送信する。

[0082] 尚、ノード50, 51に割り当てられた秘密鍵SA自体を、暗号化ピースを暗号化するための暗号鍵として用いる必要は必ずしもなく、例えば、ノード50, 51が生成した乱数RAを用いて、ハッシュ値 $H(SA || RA)$ を計算してこれを暗号鍵としても良いし、関数により暗号鍵 $F(SA, RA)$ を計算しても良い。この場合、ノード50, 51は、暗号鍵の計算に用いた乱数RAも、ピース要求を送信した他のノード51に送信する。当該他のノード51は、暗号化ピー

スを更に暗号化してその他のノード 5 1 に送信する場合、当該暗号化ピースと共に受信した乱数と自身が生成した乱数とをあわせてその他のノード 5 1 に送信する。

- [0083] また、ノード 5 0, 5 1 は暗号化ピース全体を暗号化する必要は必ずしもなく、暗号化ピースの一部分のみを暗号化しても良い。この場合、ノード 5 0, 5 1 は、暗号化ピースのどの部分を暗号化したかに関する情報（例えば、暗号化ピースの先頭(0 番目のデータとする)から 3 2 バイト分のデータを暗号化した場合には(0, 31)) を他のノード 5 1 に送信する。当該他のノード 5 1 は、暗号化ピースを更に暗号化してその他のノード 5 1 に送信する場合、当該暗号化ピースと共に受信した、暗号化ピースのどの部分を暗号化したかに関する情報と自身が暗号化ピースのどの部分を暗号化したかに関する情報をあわせてその他のノード 5 1 に送信する。この際、暗号化ピースに暗号化を行ったノード 5 0, 5 1 の順番が分かるように、例えば、ノード 5 1 A の次にノード 5 1 B が暗号化したことが分かるように、暗号化ピースのどの部分を暗号化したかに関する情報を順番に並べていく。ここで、例えば、ピースの長さを 1 2 8 バイトとして、配信開始ノードであるノード 5 0 はピース全体（例えば 1 2 8 バイト分のデータ）を暗号化し、次に暗号化ピースを受信したノード 5 1 A は先頭から 1 6 バイト分のデータを暗号化し、ノード 5 1 A から暗号化ピースを受信したノード 5 1 B は先頭から 1 6 バイト飛ばした次の 1 6 バイトのデータを暗号化する、というように暗号化ピースを受信した順番によってデータのどの部分を暗号化するかを予め定めるようにしても良い。この場合、暗号化ピースのどの部分を暗号化したかに関する情報に代えて、暗号化ピースがいくつかのノードを経由してきたかに関する情報を用いれば良い。この情報は、ノード 5 1 が暗号化ピースを受信したノードが、例えば配信開始ノードである場合 ‘0’ であり、ノード 5 1 A である場合 ‘1’、ノード 5 1 B である場合 ‘2’ である。例えば、ノード 5 1 B は、ノード 5 1 A から暗号化ピースを受信すると、この情報を ‘1’ から ‘2’ に上書きする。

- [0084] また、ピースを複数の暗号鍵で多重に暗号化する場合、ノード50, 51が鍵サーバ53へ送信する上述の要求メッセージには、暗号化ピースが経由してきた全てのノードのノードIDを含ませる。また、上述のように暗号鍵の生成に乱数を用いる場合、上述の要求メッセージには暗号化ピースが経由してきた全てのノードの乱数を含ませる。同様に、暗号化ピースのどの部分を暗号化したかに関する情報が含まれていても良いし、暗号化ピースがいくつかのノードを経由してきたかに関する情報を含んでいても良い。
- [0085] 一方、ピースを複数の暗号鍵で多重に暗号化する場合の鍵サーバ53は以下の通りである。鍵サーバ53は、上述の実施の形態と同様に、各ノード50, 51に割り当てられた秘密鍵を保持している。鍵サーバ53は、ノード51から要求メッセージを受信すると、暗号化ピースが経由してきた全てのノード50, 51のノードIDから、暗号化ピースが経由してきた各ノード50, 51に割り当てられた秘密鍵を検索し、これらを鍵束として取得する。上述のように暗号鍵の生成に乱数を用いる場合、鍵サーバ53は、暗号化ピースが経由してきた各ノード50, 51に割り当てられた秘密鍵と、それに対応するノードの乱数とを用いて復号鍵を各々計算し（上述の例においては $H(SA||A)$ 又は $F(SA, RA)$ である）、計算結果を鍵束として取得する。尚、鍵サーバ53が各ノード50, 51に割り当てられた秘密鍵を保持している必要は必ずしもなく、例えば、ノード50, 51（ノードIDの値をLIDAとする）に割り当てられた秘密鍵が ' $SA=H(Kmaster||LIDA)$ 又は $SA=F(Kmaster, LIDA)$ ' と定められている場合、鍵サーバ53はKmasterの値と関数H又はFのアルゴリズムのみを知っていれば良く、要求メッセージに含まれているLIDからそのノードIDの対応するノード50, 51に割り当てられた秘密鍵を計算することができる。
- [0086] 次に、このようなコンテンツ配信システムの構成において、本実施の形態にかかる構成を適用する例について説明する。例えば、ノード51は、他のノード51からピース要求を受信すると、送信対象の暗号化ピースに対して行われた暗号化の回数が所定回数以上である場合に、当該暗号化ピースに対

して上述の変換を行い1回の暗号化を行った後に当該暗号化ピースを他のノード51に送信する。具体的には、ノード51は、送信対象の暗号化ピースと対応付けて記憶したノードIDの数が所定数以上であるか否かを判定し、当該ノードIDの数が所定数以上である場合に、上述の実施の形態と同様にして乱数を生成して対称鍵及び変換パラメータを生成し、当該暗号化ピースに対して上述の実施形態と同様の変換を行い、生成した対称鍵を用いて、変換後の暗号化ピースを暗号化して、新たな暗号化ピースを出力する。そして、ノード51は、当該暗号化ピースと対応付けて記憶したノードID及び自身に割り当てられたノードIDと、自身が生成した乱数と、新たな暗号化ピースとを他のノード51に送信し、これらとは別に、自身が生成した対称鍵を他のノード51に送信する。一方、他のノード51は、受信した暗号化ピースをノードID、乱数及び対称鍵と対応付けて記憶する。当該他のノード51がその他のノード51に暗号化ピースを送信する場合には、当該他のノード51は、上述の実施の形態と同様にして乱数を生成して対称鍵及び変換パラメータを生成し、当該暗号化ピースと対応付けられて記憶された対称鍵を用いて当該暗号化ピースを1回復号し、復号した暗号化ピースに対して上述の実施形態と同様の変換を行い、生成した対称鍵を用いて、変換後の暗号化ピースを暗号化して、新たな暗号化ピースを出力する。そして、当該他のノード51は、当該暗号化ピースと対応付けて記憶したノードID及び自身に割り当てられたノードIDと、自身が生成した乱数と、新たな暗号化ピースとをその他のノード51に送信し、これらとは別に、自身が生成した対称鍵をその他のノード51に送信する。

[0087] 以上のような構成によれば、ピースの暗号化を3回以上重ねて行うコンテンツ配信システムにおいて、暗号化の回数を一定の回数以下に抑えることができるため、ピースの復号の際の復号の回数も一定の回数以下に抑えることができる。従って、多重に暗号化することによる安全性の向上と、復号の際の計算の効率の向上とを両立させることができる。

[0088] 尚、ピースを3回以上多重に暗号化する場合、ノード50, 51から送信さ

れる度にはなく、各ノード50, 51において、暗号化ピースに暗号化を重ねるか否かが所定の確率に従って決定されて、当該暗号化ピースについての更なる暗号化が選択的に行われるようにしても良い。このようなコンテンツ配信システムに本実施の形態にかかる構成を適用する場合、例えば、ノード51は、送信対象の暗号化ピースと対応付けて記憶したノードIDの数に所定の確率を乗算した値が所定数以上であるか否かを判定し、当該値が所定数以上である場合に、上述の実施の形態と同様にして乱数を生成して対称鍵及び変換パラメータを生成し、当該暗号化ピースに対して上述の実施形態と同様の変換を行い、生成した対称鍵を用いて、変換後の暗号化ピースを暗号化して、新たな暗号化ピースを出力すれば良い。

[0089] 上述の実施の形態においては、各ピースは、配信開始ノードであるノード50によって暗号化された後、変換パラメータを用いて変換され、変換された暗号化されたピースを受信したノード51によって、変換パラメータを用いて変換された後、対称鍵を用いて暗号化されるようにした。しかし、各ノード50, 51は、各ピースを暗号化せずに上述の変換のみ行うようにしても良い。この場合、各ノード50, 51は、対称鍵を生成することなく、変換したピースを、上述のノードID列及び乱数列と共に他のノード51に送信する。また、鍵サーバ53は、上述の実施形態と同様に鍵要求をノード51から受信すると、対称鍵を生成することなく、上述と同様にして集約パラメータを生成して、当該集約パラメータを含む復号情報を当該ノード51に対して送信する。そして、各ノード51は、復号情報に含まれる集約パラメータを用いて、ピースを逆変換すれば良い。

符号の説明

[0090] 50, 51, 51A, 51B ノード
53 鍵サーバ
500 固有情報格納部
501 乱数生成部
502 対称鍵生成部

- 5 0 3 ピース暗号化部
- 5 0 4 ピース化部
- 5 0 5 データ送信部
- 5 0 6 送信要求受付部
- 5 0 7 パラメータ生成部
- 5 0 8 変換部
- 5 1 0 固有情報格納部
- 5 1 1 乱数生成部
- 5 1 2 対称鍵生成部
- 5 1 3 ピース暗号化部
- 5 1 4 データ受信部
- 5 1 5 データ送信部
- 5 1 6 送信要求受付部
- 5 1 7 データ格納部
- 5 1 8 送信要求送信部
- 5 1 9 鍵要求送信部
- 5 2 0 ピース復号部
- 5 2 1 変換部
- 5 2 2 逆変換部
- 5 2 3 パラメータ生成部
- 5 3 0 秘密鍵格納部
- 5 3 1 データ受信部
- 5 3 2 パラメータ生成部
- 5 3 3 対称鍵生成部
- 5 3 4 データ送信部

請求の範囲

[請求項1]

データの一部であるピースを送信する通信装置であって、
他の通信装置によって可逆に変換された第1ピースと、当該他の通信装置に割り当てられた第1装置識別情報と、当該他の通信装置によって生成された第1一時情報とを受信する受信手段と、
前記第1ピースと、前記第1装置識別情報と、前記第1一時情報とを対応付けて記憶する第1記憶手段と、
当該通信装置に割り当てられた第2装置識別情報を記憶する第2記憶手段と、
その生成毎に異なり得る第2一時情報を生成する第1生成手段と、
前記第2一時情報を用いて、前記第1ピースを変換して、第2ピースを出力する変換手段と、
前記第2ピースと、前記第1装置識別情報と、前記第2装置識別情報と、前記第1一時情報と、前記第2一時情報とを送信する送信手段とを備える
ことを特徴とする通信装置。

[請求項2]

前記第2一時情報を用いて、変換を行う際に用いる変換パラメータを生成する第2生成手段を更に備え、
前記変換手段は、各変換パラメータを1つの値に集約した変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能である可逆な変換を、復号された前記第1暗号化ピースに対して、前記第2生成手段が生成した前記変換パラメータを用いて行う
ことを特徴とする請求項1に記載の通信装置。

[請求項3]

前記変換手段は、
各変換パラメータが $k_1, \dots, k_m$ ($m: 2$ 以上の自然数)であり、各変換パラメータ $k_1, \dots, k_m$ が関数 H により1つの値に集約され、集約された

変換パラメータが $H(k_1, \dots, k_m)$ であるとき、

$$L(k_1) \cdots L(k_m) = L(H(k_1, \dots, k_m))$$

を満たす関数 L により変換を、前記第1ピースに対して、前記第2生成手段が生成した前記変換パラメータ k_i ($1 \leq i \leq m$)を用いて行うことを特徴とする請求項2に記載の通信装置。

[請求項4] 前記第1ピースは、前記他の通信装置によって可逆に変換され且つ暗号化されており、

前記受信手段は、前記第1ピースと、前記第1装置識別情報と、前記第1一時情報と、前記第1一時情報を用いて生成され前記第1ピースの暗号化に用いられた第1対称鍵とを受信し、

前記第1記憶手段は、前記第1ピースと、前記第1装置識別情報と、前記第1一時情報と、前記第1対称鍵とを対応付けて記憶し、

前記第2一時情報を用いて、第2対称鍵を生成する第3生成手段と、

前記第1ピースと対応付けられて記憶された前記第1対称鍵を用いて、当該第1ピースを復号する第1復号手段と、

前記第2一時情報を用いて、復号された前記第1暗号化ピースを変換する変換手段と、

変換された前記第1ピースを、前記第2対称鍵を用いて暗号化して、前記第2ピースを出力する暗号化手段とを更に備え、

前記送信手段は、前記第2ピースと、前記第1装置識別情報と、前記第2装置識別情報と、前記第1一時情報と、前記第2一時情報と、前記第2対称鍵とを送信する

ことを特徴とする請求項2又は3に記載の通信装置。

[請求項5] 前記第1生成手段は、2つの前記第2一時情報を生成し、

前記第2生成手段は、2つの前記第2一時情報のうち他方を用いて、前記変換パラメータを生成し、

前記第3生成手段は、2つの前記第2一時情報のうち一方を用いて

、前記第 2 対称鍵を生成する

ことを特徴とする請求項 3 又は 4 に記載の通信装置。

[請求項 6] 前記第 2 記憶手段は、当該通信装置に一意に割り当てられている秘密情報を更に記憶し、

前記第 3 生成手段は、前記第 2 一時情報と前記秘密情報とを用いて前記対称鍵を生成する

ことを特徴とする請求項 4 に記載の通信装置。

[請求項 7] 前記第 2 生成手段は、前記第 2 一時情報と前記秘密情報とを用いて前記変換パラメータを生成する

ことを特徴とする請求項 5 に記載の通信装置。

[請求項 8] 前記受信手段は、前記第 1 ピース、前記第 1 装置識別情報及び前記第 1 一時情報と、前記第 1 対称鍵とを異なるタイミングで受信することを特徴とする請求項 4 乃至 7 のいずれか一項に記載の通信装置。

[請求項 9] 前記変換パラメータを暗号化して第 3 記憶手段に記憶させる第 1 記憶制御手段を更に備える

ことを特徴とする請求項 2 乃至 8 のいずれか一項に記載の通信装置。

[請求項 10] 前記第 1 対称鍵を暗号化して、前記第 1 ピース、前記第 1 装置識別情報及び前記第 1 一時情報とを対応付けて前記第 1 記憶手段に記憶させること及び前記第 2 対称鍵を暗号化して第 4 記憶手段に記憶させることのうち少なくとも一方を行う第 2 記憶制御手段を更に備えることを特徴とする請求項 4 乃至 9 のいずれか一項に記載の通信装置。

[請求項 11] 前記ピースを要求するピース要求を受信する要求受信手段を更に備え、

前記第 1 生成手段は、前記ピース要求が受信された場合に、前記第 2 一時情報を生成する

ことを特徴とする請求項 1 乃至 10 のいずれか一項に記載の通信装置。

[請求項 12] データの一部であるピースを受信する通信装置であって、

当該通信装置に割り当てられている装置識別情報を記憶する第 1 記憶手段と、

他の通信装置によって可逆に変換されたピースと、当該他の通信装置に割り当てられている装置識別情報と、当該他の通信装置によって生成された一時情報とを受信する第 1 受信手段と、

前記ピース、前記装置識別情報及び前記一時情報を対応付けて記憶する第 2 記憶手段と、

前記ピースを逆変換するための復号情報を要求すると共に、当該ピースと対応付けられて記憶された前記装置識別情報及び前記一時情報を対応付けて含む鍵要求を鍵サーバへ送信する送信手段と、

前記鍵要求に応じて前記鍵サーバから、前記復号情報を受信する第 2 受信手段と、

受信された前記復号情報を用いて前記ピースを逆変換する逆変換手段とを備える

ことを特徴とする通信装置。

[請求項13]

前記ピースは、可逆に変換され且つ暗号化されており、

前記第 1 受信手段は、前記他の通信装置によって、前記一時情報を用いて生成された変換パラメータを用いて変換された後、前記一時情報を用いて生成された対称鍵を用いて暗号化された前記ピースと、前記装置識別情報と、前記一時情報とを受信する

ことを特徴とする請求項 1 2 に記載の通信装置。

[請求項14]

前記一時情報は、前記他の通信装置によって 2 つ生成され、

前記第 1 受信手段は、前記他の通信装置によって、2 つの前記一時情報のうち一方を用いて生成された変換パラメータを用いて変換された後、2 つの前記一時情報のうち他方を用いて生成された対称鍵を用いて暗号化された前記ピースと、前記装置識別情報と、2 つの前記一時情報とを受信する

ことを特徴とする請求項 1 3 に記載の通信装置。

[請求項15] 前記ピースは、ピースを最初に暗号化するその他の通信装置によって、第1対称鍵を用いて暗号化された後、第1変換パラメータを用いて変換され、前記他の通信装置によって、第2変換パラメータを用いて変換された後、第2対称鍵を用いて暗号化されており、

前記暗号化ピースに対して行われた変換は、各変換パラメータを1つの値に集約した変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能なものであり、

前記第1受信手段は、前記ピースと、前記その他の通信装置の前記装置識別情報及び前記他の通信装置の前記装置識別情報と、前記その他の通信装置が生成した前記一時情報及び前記他の通信装置が生成した前記一時情報と、前記第2対称鍵とを受信し、

前記第2受信手段は、前記第1変換パラメータ及び前記第2変換パラメータが集約された変換パラメータと、前記第1対称鍵とを含む前記復号情報を前記鍵サーバから受信する

ことを特徴とする請求項13又は14に記載の通信装置。

[請求項16] 前記第2受信手段は、前記第2対称鍵を更に含む前記復号情報を前記鍵サーバから受信する

ことを特徴とする請求項15に記載の通信装置。

[請求項17] 前記逆変換手段は、

前記第1対称鍵を用いて、前記ピースを復号する第1ピース復号手段と、

前記復号情報に含まれる前記変換パラメータを用いて、復号された前記ピースを逆変換するピース逆変換手段と、

前記第2対称鍵を用いて、逆変換された前記ピースを復号する第2ピース復号手段とを有する

ことを特徴とする請求項15又は16に記載の通信装置。

[請求項18] データの一部であるピースを送信する複数の他の通信装置のそれぞ

れに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶する第 1 記憶手段と、

可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第 1 通信装置から受信する受信手段と、

前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する第 1 生成手段と、

前記変換パラメータを含む前記復号情報を前記第 1 通信装置に送信する送信手段とを備える

ことを特徴とするサーバ。

[請求項19]

前記ピースに対して行われた変換は、各変換パラメータを 1 つの値に集約された変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能なものであり、

前記第 1 生成手段は、

前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、前記変換パラメータを前記装置識別情報毎に各々生成する第 1 パラメータ生成手段と、

生成された各前記変換パラメータを、当該各変換パラメータを用いて各変換を重ねて行った結果と、当該各変換パラメータを 1 つの値に集約した変換パラメータを用いて変換を行った結果とが同一となるように、1 つの値に集約する集約手段とを有し、

前記送信手段は、集約された前記変換パラメータを含む前記復号情

報を前記第 1 通信装置に送信する

ことを特徴とする請求項 18 に記載のサーバ。

[請求項20]

前記ピースは、可逆に変換され且つ暗号化されており、

前記複数の他の通信装置のうち前記ピースを最初に暗号化した第 2 通信装置が生成した前記一時情報と、当該第 2 の通信装置に対応する前記秘密情報とを用いて、第 1 対称鍵を生成する第 2 生成手段を更に備え、

前記送信手段は、前記変換パラメータ及び前記第 1 対称鍵を含む前記復号情報を前記第 1 通信装置に送信する

ことを特徴とする請求項 18 又は 19 に記載のサーバ。

[請求項21]

前記複数の他の通信装置のうち前記ピースを最後に暗号化した第 3 通信装置が生成した前記一時情報及び当該第 3 通信装置に対応する前記秘密情報を用いて、第 2 対称鍵を生成する第 3 生成手段を更に備え、

前記送信手段は、前記変換パラメータ、前記第 1 対称鍵及び前記第 2 対称鍵を含む前記復号情報を前記第 1 通信装置に送信する

ことを特徴とする請求項 20 に記載のサーバ。

[請求項22]

前記一時情報は、前記複数の他の通信装置毎に各々複数生成され、

前記複数の他の通信装置の各々において、前記一時情報のうち 1 つを用いて前記対称鍵が生成され、

前記複数の他の通信装置の各々において、前記一時情報のうち前記対称鍵の生成に用いられていない一時情報を用いて前記変換パラメータが生成され、

前記第 1 生成手段は、前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる前記一時情報のうち前記変換パラメータの生成に用いられた前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成し、

前記第 2 生成手段は、前記第 2 通信装置が前記第 1 対称鍵の生成に用いた前記一時情報と、当該第 2 の通信装置に対応する前記秘密情報とを用いて、前記第 1 対称鍵を生成することを特徴とする請求項 20 又は 21 に記載のサーバ。

[請求項 23]

データの一部であるピースを送信する通信装置で実行される通信方法であって、

他の通信装置によって可逆に変換された第 1 ピースと、当該他の通信装置に割り当てられた第 1 装置識別情報と、当該他の通信装置によって生成された第 1 一時情報とを受信する受信ステップと、

前記第 1 ピースと、前記第 1 装置識別情報と、前記第 1 一時情報とを対応付けて記憶手段に記憶させる記憶制御ステップと、

その生成毎に異なり得る第 2 一時情報を生成する生成ステップと、

前記第 2 一時情報を用いて、前記第 1 ピースを変換して、第 2 ピースを出力する変換ステップと、

前記第 2 ピースと、前記第 1 装置識別情報と、前記第 2 装置識別情報と、前記第 1 一時情報と、前記第 2 一時情報とを送信する送信ステップとを含む

ことを特徴とする通信方法。

[請求項 24]

データの一部であるピースを送信する通信装置の有するコンピュータに実行させるためのプログラムであって、

他の通信装置によって可逆に変換された第 1 ピースと、当該他の通信装置に割り当てられた第 1 装置識別情報と、当該他の通信装置によって生成された第 1 一時情報とを受信する受信ステップと、

前記第 1 ピースと、前記第 1 装置識別情報と、前記第 1 一時情報とを対応付けて記憶手段に記憶させる記憶制御ステップと、

その生成毎に異なり得る第 2 一時情報を生成する生成ステップと、

前記第 2 一時情報を用いて、前記第 1 ピースを変換して、第 2 ピースを出力する変換ステップと、

前記第 2 ピースと、前記第 1 装置識別情報と、前記第 2 装置識別情報と、前記第 1 一時情報と、前記第 2 一時情報とを送信する送信ステップとをコンピュータに実行させるプログラム。

[請求項25]

データの一部であるピースを送信する複数の他の通信装置のそれぞれに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶するサーバの有するコンピュータに実行させるためのプログラムであって、

可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第 1 通信装置から受信する受信ステップと、

前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する生成ステップと、

前記変換パラメータを含む前記復号情報を前記第 1 通信装置に送信する送信ステップとをコンピュータに実行させるプログラム。

補正された請求の範囲
[2010年2月1日 (01.02.2010) 国際事務局受理]

[1] データの一部であるピースを送信する通信装置であって、

他の通信装置によって可逆に変換された第 1 ピースと、当該他の通信装置に割り当てられた第 1 装置識別情報と、当該他の通信装置によって生成された第 1 一時情報とを受信する受信手段と、

前記第 1 ピースと、前記第 1 装置識別情報と、前記第 1 一時情報とを対応付けて記憶する第 1 記憶手段と、

当該通信装置に割り当てられた第 2 装置識別情報を記憶する第 2 記憶手段と、

その生成毎に異なり得る第 2 一時情報を生成する第 1 生成手段と、

前記第 2 一時情報を用いて、前記第 1 ピースを変換して、第 2 ピースを出力する変換手段と、

前記第 2 ピースと、前記第 1 装置識別情報と、前記第 2 装置識別情報と、前記第 1 一時情報と、前記第 2 一時情報とを送信する送信手段とを備えることを特徴とする通信装置。

[2] 前記第 2 一時情報を用いて、変換を行う際に用いる変換パラメータを生成する第 2 生成手段を更に備え、

前記変換手段は、各変換パラメータを 1 つの値に集約した変換パラメータを用いて変換を行った結果と、各変換パラメータを用いて重ねて変換を行った結果とが同一となり且つ集約された変換パラメータを用いて逆変換が可能である可逆な変換を、復号された前記第 1 暗号化ピースに対して、前記第 3 生成手段が生成した前記変換パラメータを用いて行うことを特徴とする請求項 1 に記載の通信装置。

[3] 前記変換手段は、

各変換パラメータが $k_1, \dots, k_m$ ($m: 2$ 以上の自然数) であり、各変換パラメータ $k_1, \dots, k_m$ が関数 H により 1 つの値に集約され、集約された変換パラメータが $H(k_1, \dots, k_m)$ であるとき、 $L(k_1) \cdots L(k_m) = L(H(k_1, \dots, k_m))$

を満たす関数 L により変換を、前記第1ピースに対して、前記第2生成手段が生成した前記変換パラメータ k_i ($1 \leq i \leq m$)を用いて行う

ことを特徴とする請求項2に記載の通信装置。

[4] (補正後) 前記第1ピースは、前記他の通信装置によって可逆に変換され且つ暗号化されており、

前記受信手段は、前記第1ピースと、前記第1装置識別情報と、前記第1一時情報と、前記第1一時情報を用いて生成され前記第1ピースの暗号化に用いられた第1対称鍵とを受信し、

前記第1記憶手段は、前記第1ピースと、前記第1装置識別情報と、前記第1一時情報と、前記第1対称鍵とを対応付けて記憶し、

前記第2一時情報を用いて、第2対称鍵を生成する第3生成手段と、

前記第1ピースと対応付けられて記憶された前記第1対称鍵を用いて、当該第1ピースを復号する第1復号手段と、

前記第2一時情報を用いて、復号された前記第1暗号化ピースを変換する変換手段と、

変換された前記第1ピースを、前記第2対称鍵を用いて暗号化して、前記第2ピースを出力する暗号化手段とを更に備え、

前記送信手段は、前記第2ピースと、前記第1装置識別情報と、前記第2装置識別情報と、前記第1一時情報と、前記第2一時情報と、前記第2対称鍵とを送信する

ことを特徴とする請求項2に記載の通信装置。

[5] (補正後) 前記第1生成手段は、2つの前記第2一時情報を生成し、

前記第2生成手段は、2つの前記第2一時情報のうち他方を用いて、前記変換パラメータを生成し、

前記第3生成手段は、2つの前記第2一時情報のうち一方を用いて、前記第2対称鍵を生成する

ことを特徴とする請求項3に記載の通信装置。

[6] (削除)

[7] 前記第2生成手段は、前記第2一時情報と前記秘密情報とを用いて前記変換パラメータを生成することを特徴とする請求項5に記載の通信装置。

[8] (削除)

[9] (削除)

[10] (削除)

[11] (削除)

[12] データの一部であるピースを受信する通信装置であって、
当該通信装置に割り当てられている装置識別情報を記憶する第1記憶手段と、
他の通信装置によって可逆に変換されたピースと、当該他の通信装置に割り当てられている装置識別情報と、当該他の通信装置によって生成された一時情報とを受信する第1受信手段と、
前記ピース、前記装置識別情報及び前記一時情報を対応付けて記憶する第2記憶手段と、
前記ピースを逆変換するための復号情報を要求すると共に、当該ピースと対応付けられて記憶された前記装置識別情報及び前記一時情報を対応付けて含む鍵要求を鍵サーバへ送信する送信手段と、
前記鍵要求に応じて前記鍵サーバから、前記復号情報を受信する第2受信手段と、
受信された前記復号情報を用いて前記ピースを逆変換する逆変換手段とを備えることを特徴とする通信装置。

[13] (削除)

[14] (削除)

[15] (削除)

[16] (削除)

[17] (削除)

[18] データの一部であるピースを送信する複数の他の通信装置のそれぞれに割り当てられた秘密情報と、各通信装置に割り当てられた装置識別情報とを各々対応付けて記憶する第1記憶手段と、

可逆に変換された前記ピースを逆変換するための復号情報を要求すると共に、前記複数の他の通信装置の前記装置識別情報及び当該複数の他の通信装置が各々生成した情報であってその生成毎に異なり得る一時情報とを対応付けて含む要求を第1通信装置から受信する受信手段と、

前記要求に含まれる各前記装置識別情報に対応付けられて記憶されている前記秘密情報と、当該各装置識別情報と対応付けられて前記要求に含まれる各前記一時情報とを用いて、逆変換を行う際に用いる変換パラメータを生成する第1生成手段と、

前記変換パラメータを含む前記復号情報を前記第1通信装置に送信する送信手段とを備えることを特徴とするサーバ。

[19] (削除)

[2 0] (削除)

[2 1] (削除)

[2 2] (削除)

[2 3] (削除)

[2 4] (削除)

[2 5] (削除)

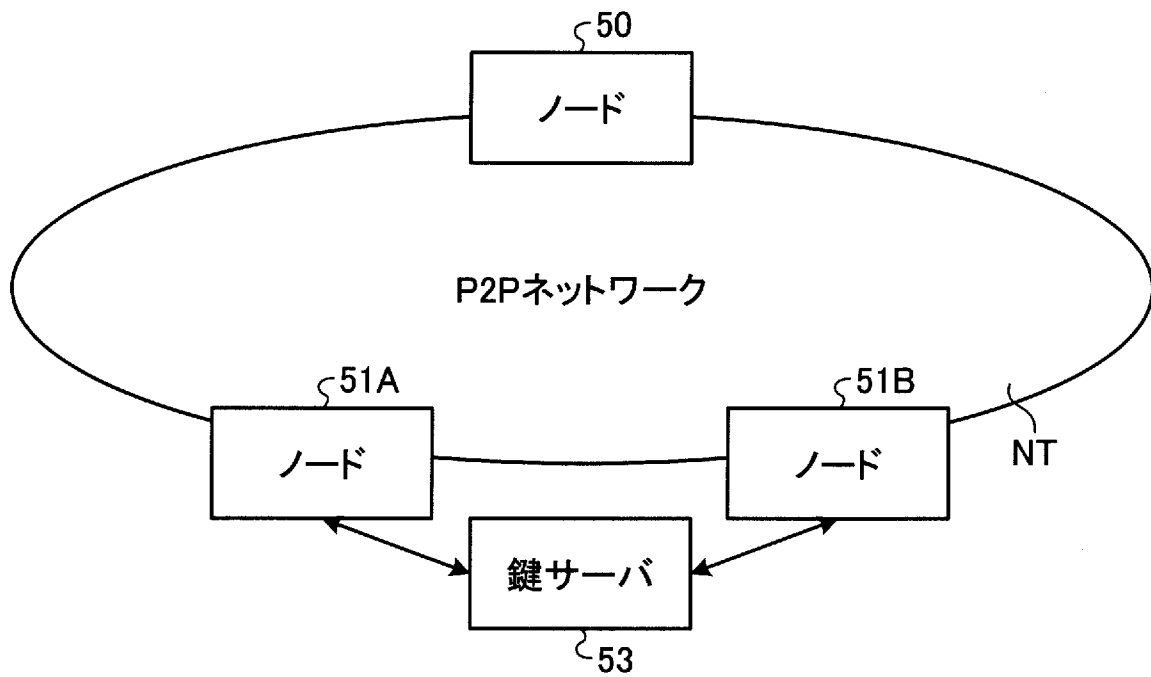
条約第19条(1)に基づく説明書

請求項4は、請求項2のみに従属させる補正を行いました。

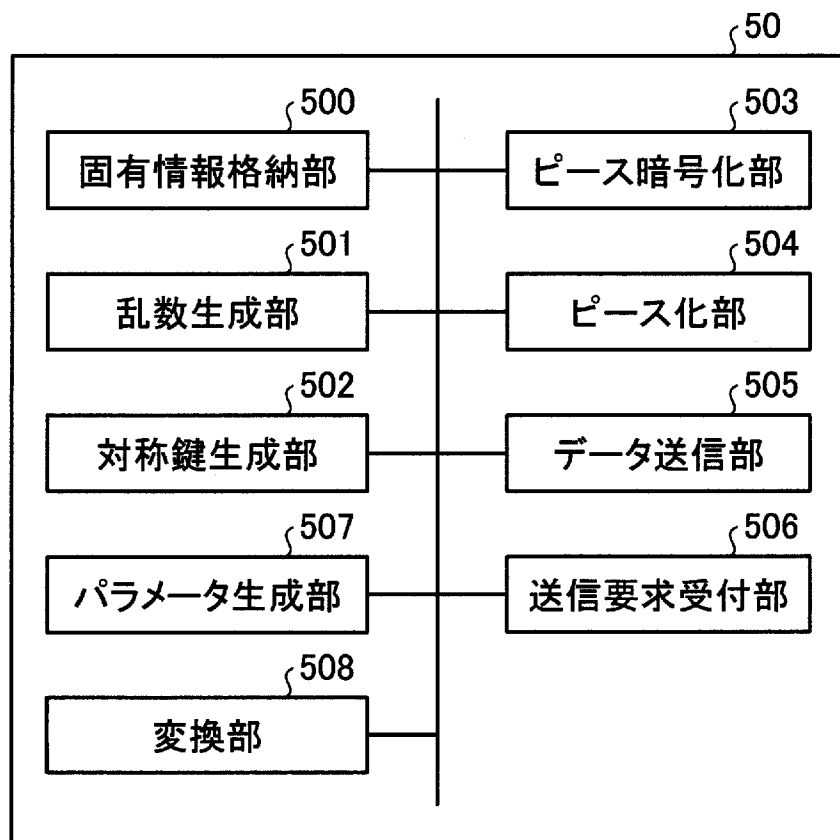
請求項5は、請求項3のみに従属させる補正を行いました。

請求項6, 8～11, 13～17, 19～25は、削除する補正を行いました。

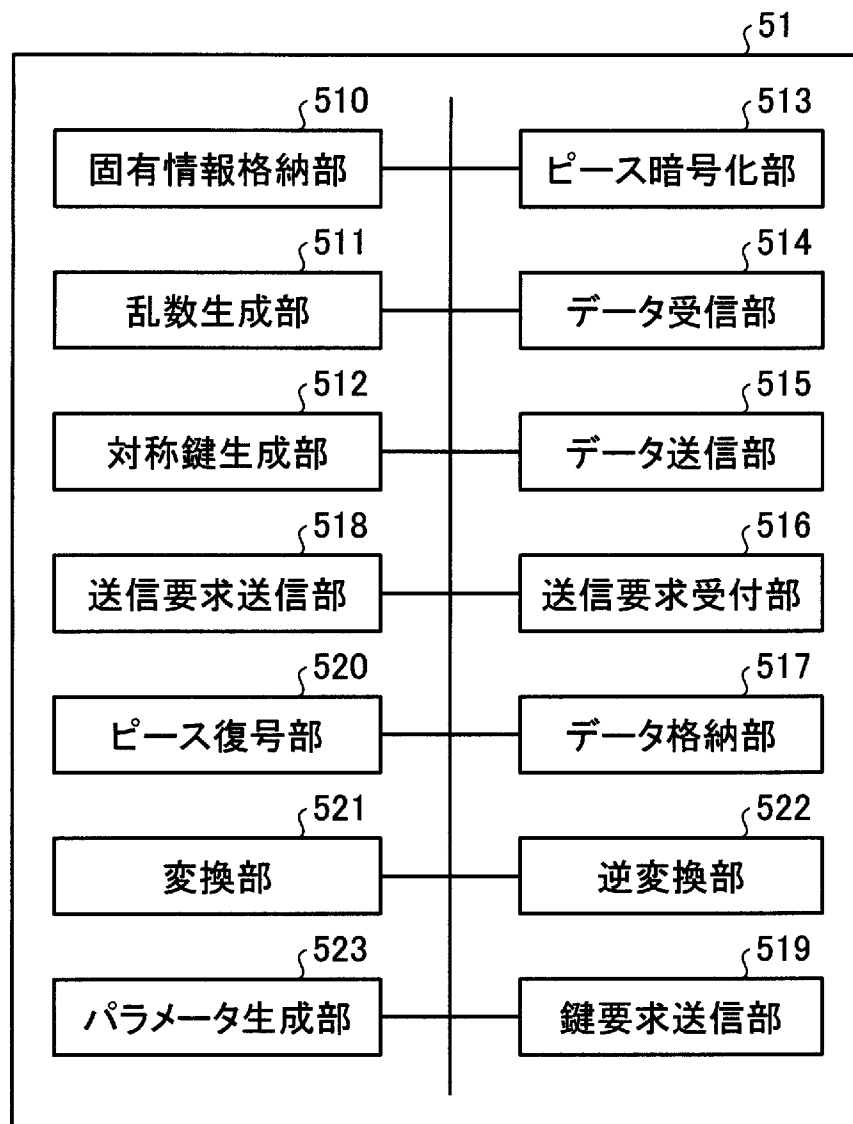
[図1]



[図2]



[図3]



[図4]

ノード50 → ノード51A

ID #0 r, r_0, r'_0 $E(k_0)L(k'_0)E(k)P$
k_0

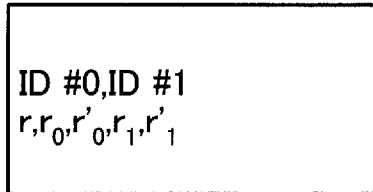
[図5]

ノード51A → ノード51B

ID #0, ID #1 r, r_0, r'_0, r_1, r'_1 $E(k_1)L(k'_1)(k'_0)E(k)P$
k_1

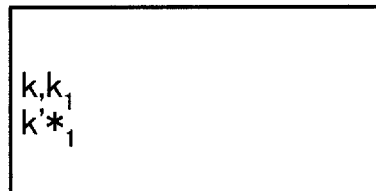
[図6]

ノード51B → 鍵サーバ53

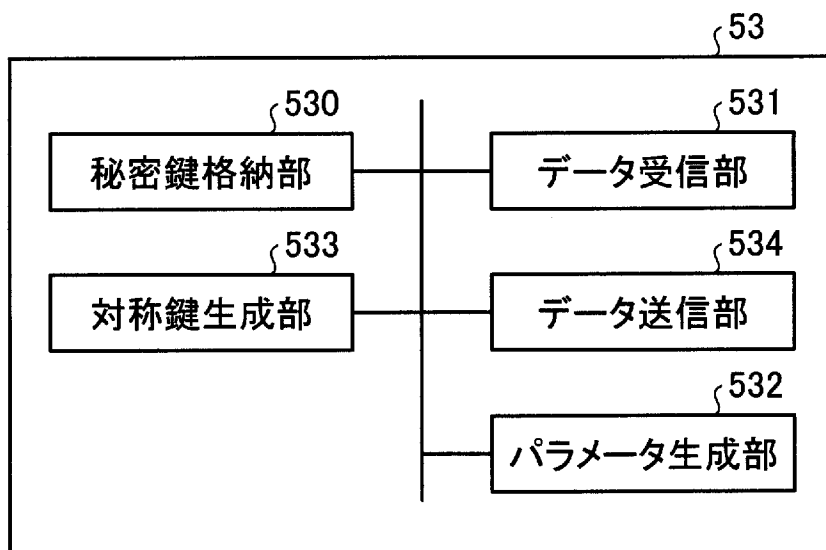


[図7]

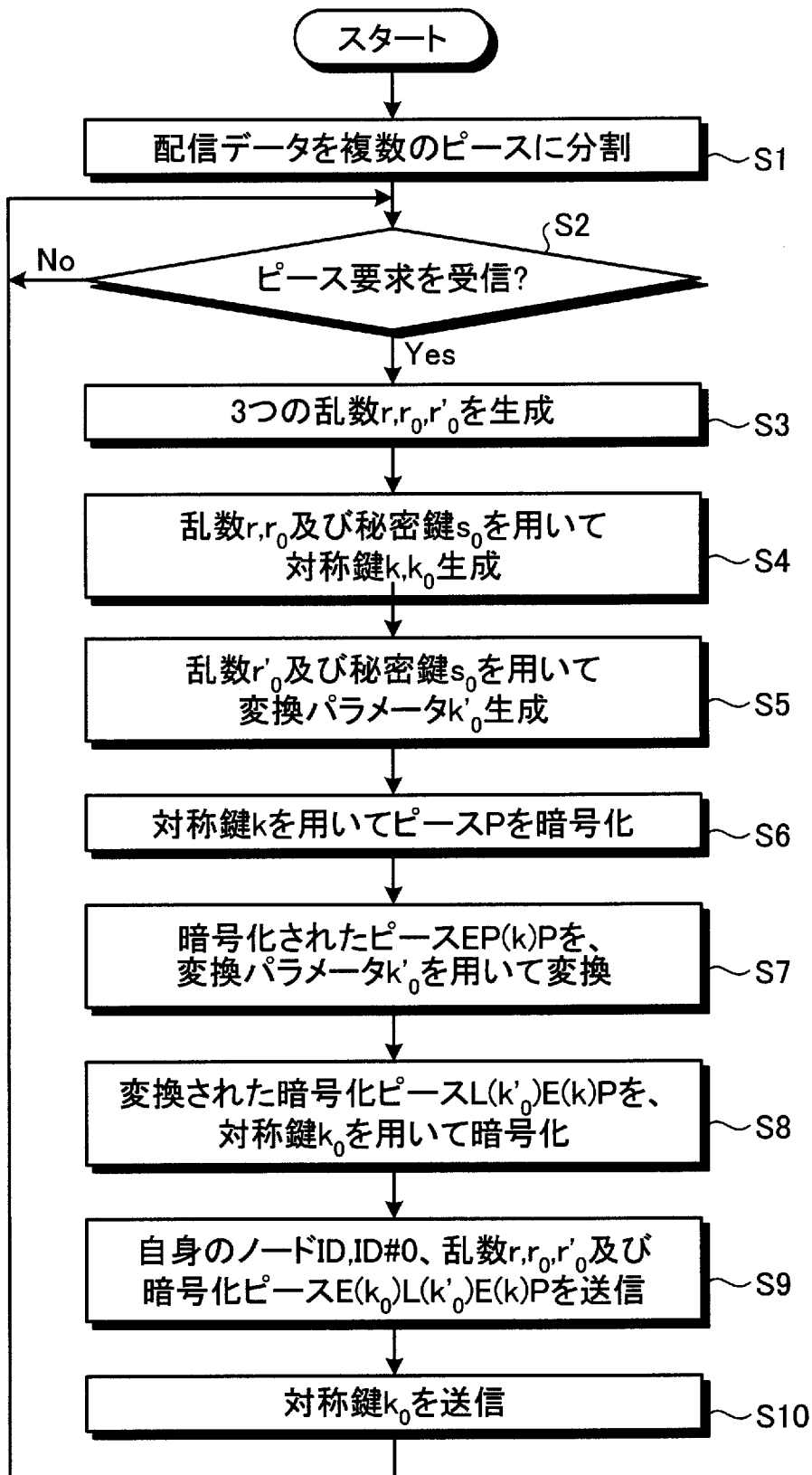
鍵サーバ53 → ノード51B



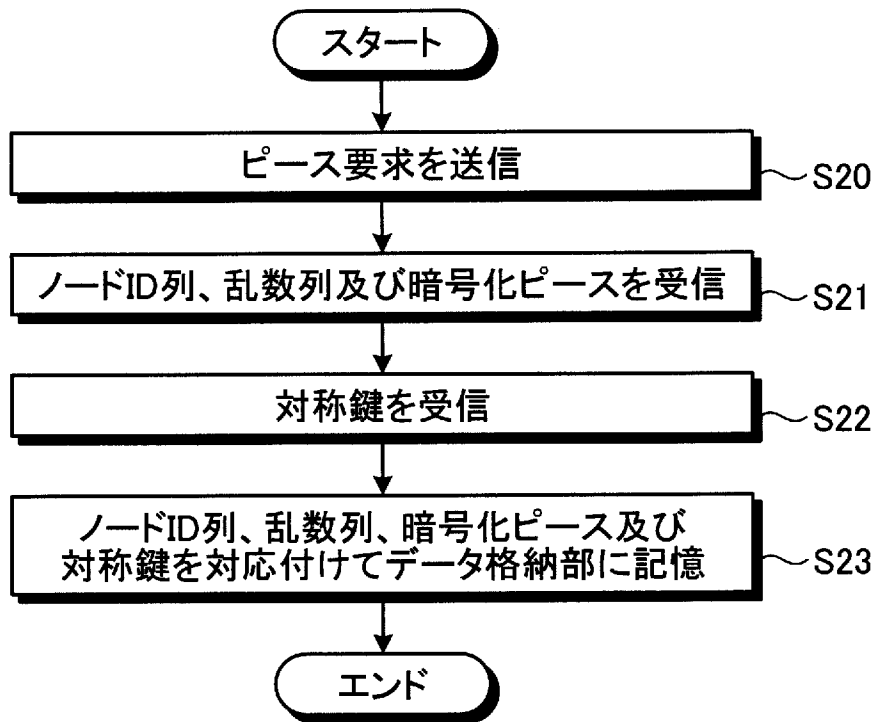
[図8]



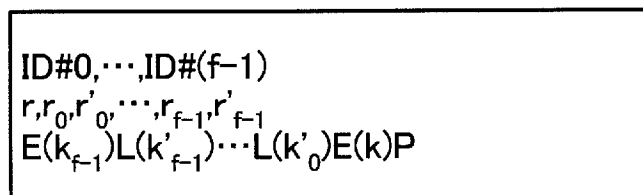
[図9]



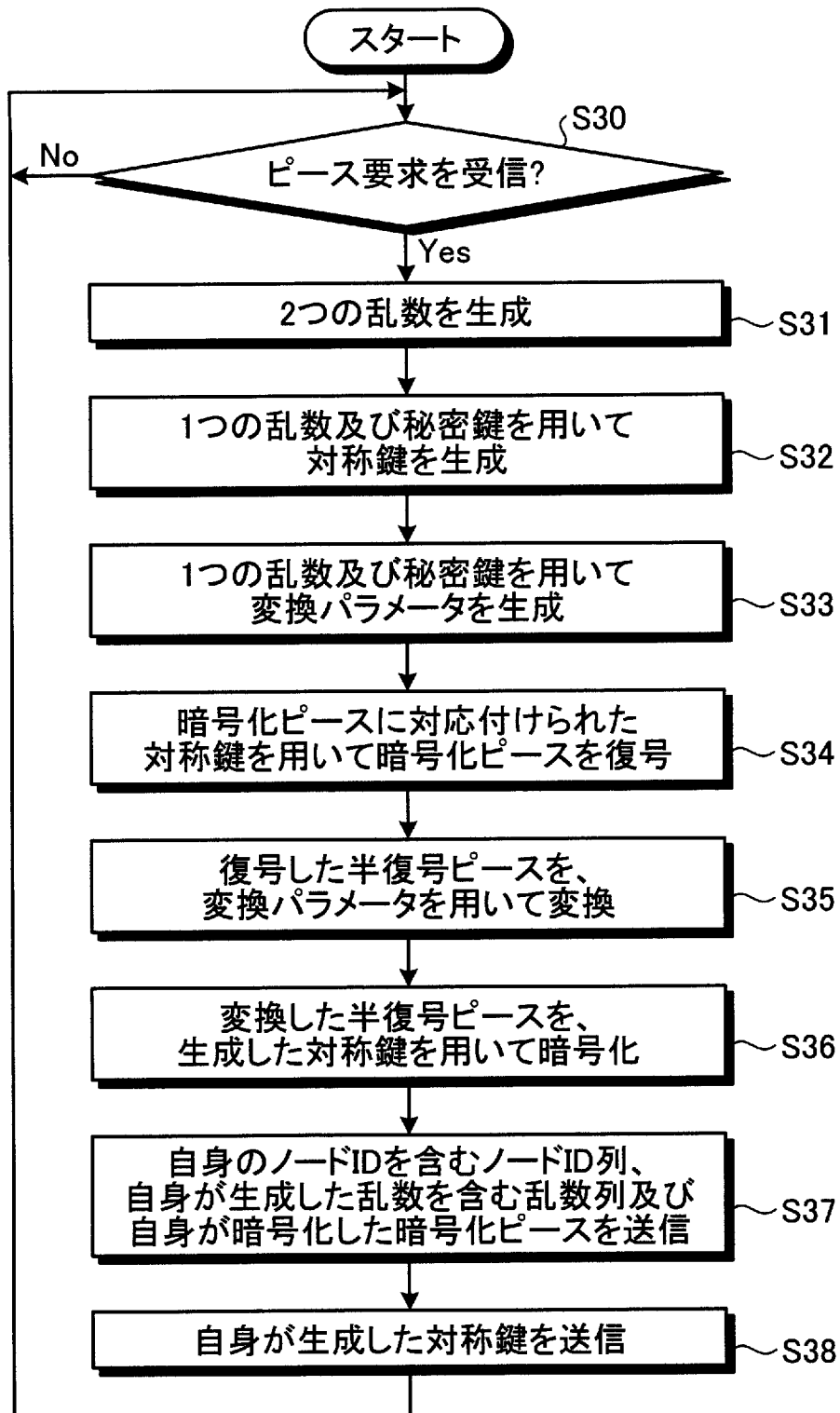
[図10]



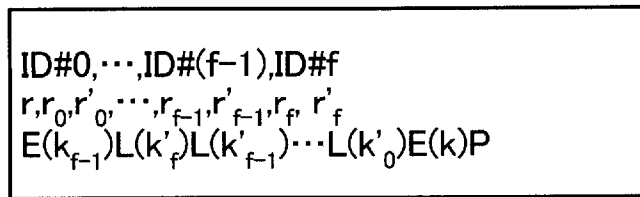
[図11]



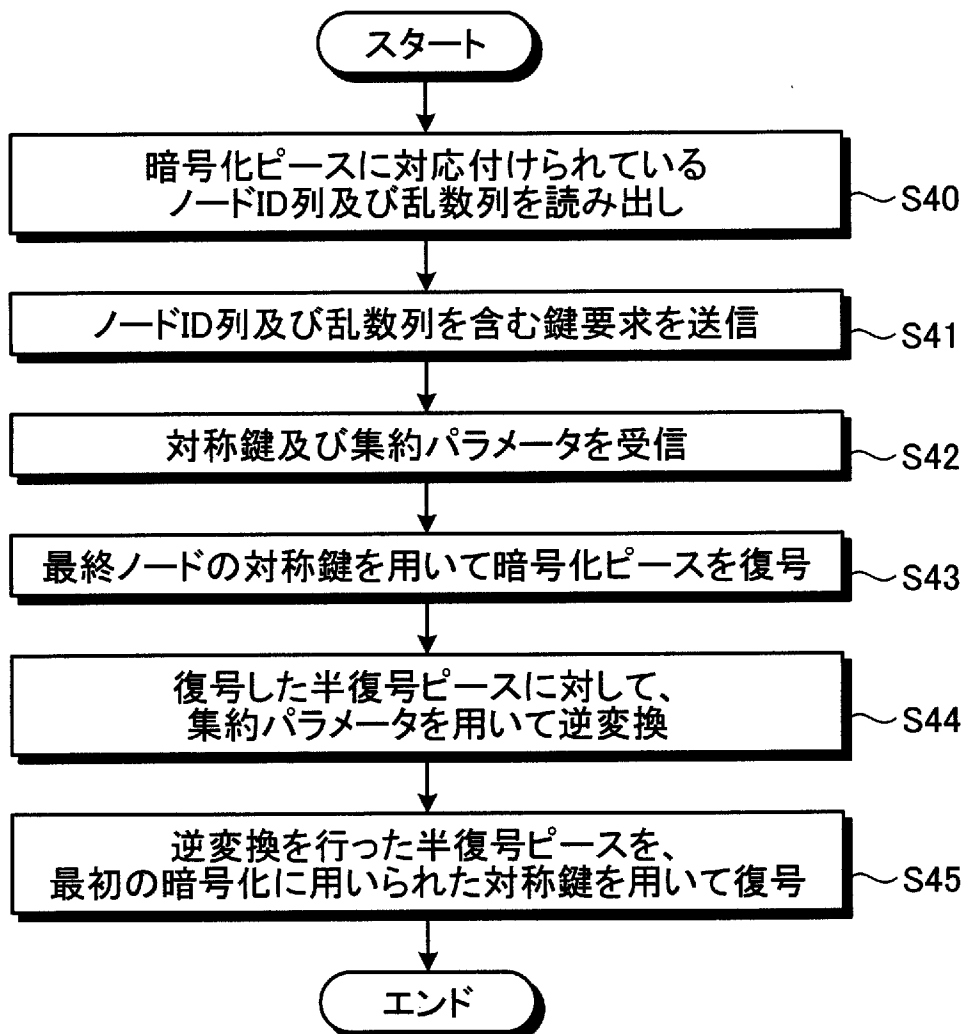
[図12]



[図13]



[図14]



[図15]

$$\text{ID\#0}, \dots, \text{ID\#(f-1)}, \text{ID\#f}$$

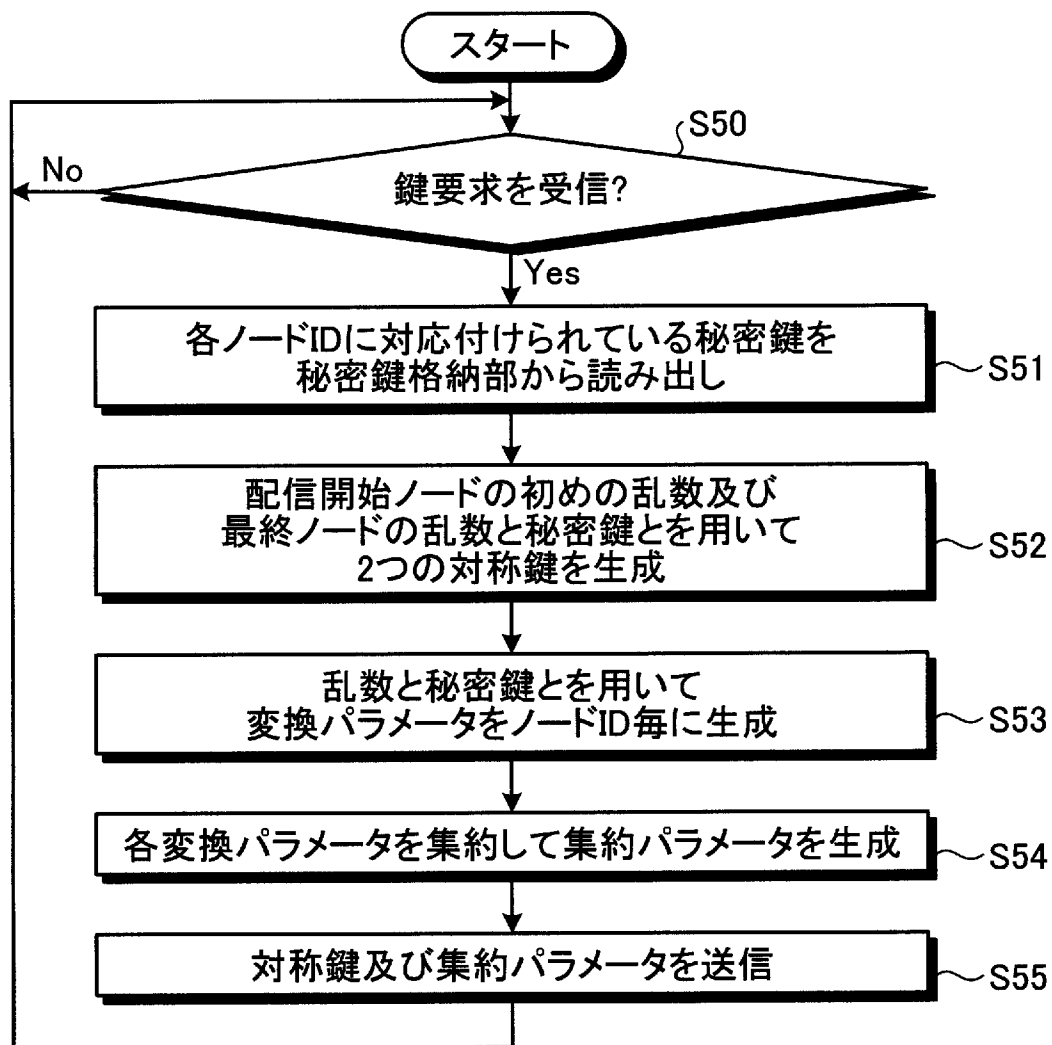
$$r, r_0, r'_0, \dots, r_{f'} r_{f'}$$

[図16]

$$k, k_{f-1}$$

$$H(k_{f-1}, \dots, k'_0)$$

[図17]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/065664

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i, H04L9/16(2006.01)i, H04L12/56(2006.01)i, H04W12/02(2009.01)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, H04L9/16, H04L12/56, H04W12/02

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	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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.
A	JP 2008-192129 A (DoCoMo Technology, Inc.), 21 August 2008 (21.08.2008), entire text; all drawings (Family: none)	1-22
A	Yuta OKAMOTO, Tomonori HIRUTA, Hayato YAMANA, "P2P File Kyoyu Network o Riyo shita Daikibo Bunsan Storage no Jitsugen", Proceedings of the 69th (Heisei 19 Nen) National Meeting of Information Processing Society of Japan (3, 06 March 2007 (06.03.2007), (3), 1W-1, pages 3-297 to 3-298	1-22



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
01 December, 2009 (01.12.09)Date of mailing of the international search report
15 December, 2009 (15.12.09)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/065664

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Yuta OKAMOTO, Hayato YAMANA, "Bunsan Meta P2P Storage 'DiMPS' ni yoru Contents Haishin System no Jitsugen", The Institute of Electronics, Information and Communication Engineers Dai 19 Kai Data Kogaku Workshop Ronbunshu, 07 April 2008 (07.04.2008), I2: Interactive Session 2, 31, pages 1 to 6, <retrieval date 01 December 2009 (01.12.2009)>	1-22
A	Yuichi JINNO, Taishi KATO, Hideyuki FUKUOKA, Mikiya TANI, "P2P Network ni Okeru Joho no Ryutsu Kanshi Hoshiki no Teian", Proceedings of the 67th (Heisei 17 Nendo) IEICE General Conference, 02 March 2005 (02.03.2005), (3), 6K-4, pages 3-99 to 3-100	1-22
E,A	Toru KANBAYASHI, Taku KATO, Tatsuyuki MATSUSHITA, Kentaro UMEZAWA, Shinji YAMANAKA, "JetJigsaw: P2P o Riyo shita Chosakuken Hogo Hoshiki no Shin Teian", 2009 Nen Symposium on Cryptography and Information Security (SCIS2009), 20 January 2009 (20.01.2009), 1B2 Contents Hogo, 1B2-2	1-22
E,A	Tatsuyuki MATSUSHITA, Kentaro UMEZAWA, Shinji NAKAYAMA, "JetJigsaw ni Okeru Piece Kaizan Kenchi Hoho no Teian", IEICE Technical Report, 02 March 2009 (02.03.2009), vol.108, no.473, pages 1 to 6, ISEC2008-101 to 188, Joho Security	1-22

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/065664

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 23-25
because they relate to subject matter not required to be searched by this Authority, namely:

See extra sheet.
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/065664

Continuation of Box No.II-1 of continuation of first sheet(2)

The inventions of claims 23-25 substantially describe an algorithm for transmitting a piece as a part of data. This is a scientific theory itself which does not require search by the International Search Authority under the provisions of PCT Article 17 (2) (a) (i) and PCT Rule 39.1.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/08(2006.01)i, H04L9/16(2006.01)i, H04L12/56(2006.01)i, H04W12/02(2009.01)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（I P C））

Int.Cl. H04L9/08, H04L9/16, H04L12/56, H04W12/02

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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 請求項の番号
A	JP 2008-192129 A（ドコモ・テクノロジー株式会社）2008.08.21, 全文, 全図（ファミリーなし）	1 - 2 2
A	岡本雄太, 蛭田智則, 山名早人, “P 2 P ファイル共有ネットワークを利用した大規模分散ストレージの実現”, 情報処理学会第 6 9 回（平成 1 9 年）全国大会講演論文集（3, 2007.03.06, （3）, 1 W - 1, p. 3・2 9 7 - 3・2 9 8	1 - 2 2

☒ 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

0 1 . 1 2 . 2 0 0 9

国際調査報告の発送日

1 5 . 1 2 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

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）

青木 重徳

5 S

4 2 2 9

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 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 請求項の番号
A	岡本雄太, 山名早人, “分散メタ P 2 P ストレージ「D i M P S」によるコンテンツ配信システムの実現”, 電子情報通信学会第 1 9 回データ工学ワークショップ論文集, 2008.04.07, I 2 : インタラクティブセッション 2, 3 1, p. 1 - 6, <検索日: 2 0 0 9 年 1 2 月 1 日>	1 - 2 2
A	仁野裕一, 加藤大志, 福岡秀幸, 谷幹也, “P 2 P ネットワークにおける情報の流通監視方式の提案”, 情報処理学会第 6 7 回 (平成 1 7 年) 全国大会講演論文集, 2005.03.02, (3), 6 K - 4, p. 3 - 9 9 - 3 - 1 0 0	1 - 2 2
E, A	上林達, 加藤拓, 松下達之, 梅澤健太郎, 山中晋爾, “JetJigsaw:P2P を利用した著作権保護方式の新提案”, 2 0 0 9 年暗号と情報セキュリティシンポジウム (SCIS2009), 2009.01.20, 1 B 2 コンテンツ保護, 1 B 2 - 2	1 - 2 2
E, A	松下達之, 梅澤健太郎, 山中晋爾, “JetJigsaw におけるピース改ざん検知方法の提案”, 電子情報通信学会技術研究報告, 2009.03.02, V o l . 1 0 8, N o . 4 7 3, p. 1 - 6, I S E C 2 0 0 8 - 1 0 1 ~ 1 8 8, 情報セキュリティ	1 - 2 2

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（P C T 17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☒ 請求項 2 3 - 2 5 は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
（特別ページ）を参照されたい。
2. ☐ 請求項 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求項 _____ は、従属請求の範囲であってP C T 規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

請求項 23-25 は、実質的にはデータの一部であるピースを送信するためのアルゴリズムを記載したものであるから、科学の理論そのものであり PCT 第 17 条 (2) (a) (i) 及び PCT 規則 39.1 の規定により、この国際調査機関が調査することを要しない対象に係るものである。