

(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
2013 年 1 月 31 日(31.01.2013)



(10) 国際公開番号
WO 2013/015252 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01)
- (21) 国際出願番号: PCT/JP2012/068614
- (22) 国際出願日: 2012 年 7 月 23 日(23.07.2012)
- (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 2011-161118 2011 年 7 月 22 日(22.07.2011) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ(NTT DOCOMO, INC.) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目 1 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): 山森 修 (YAMAMORI, Osamu) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP).
- (74) 代理人: 特許業務法人朝日特許事務所 (ASAHI PATENT FIRM); 〒1010054 東京都千代田区神田錦町三丁目 1 5 番地 NTF 竹橋ビル 3 階 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, JP, 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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

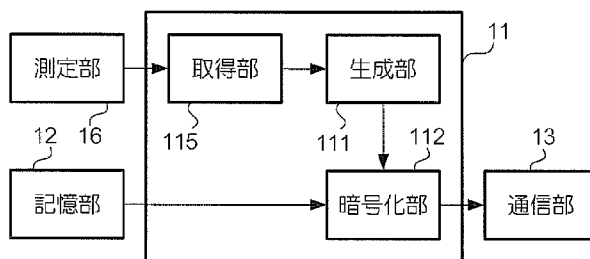
添付公開書類:

— 国際調査報告 (条約第 21 条(3))

(54) Title: INFORMATION TRANSMISSION TERMINAL

(54) 発明の名称: 情報伝送端末

[図3]



- 12 Storage unit
13 Communication unit
16 Measurement unit
111 Generation unit
112 Encryption unit
115 Acquisition unit

(57) Abstract: [Problem] To make it difficult to predict a key which is used in an encrypted communication. [Solution] With a transmission-side information transmission terminal (1), a measurement unit (16) measures quantities of a plurality of respective components which are included in a specimen. An acquisition unit (115) acquires information which denotes the quantities of the components which are measured by the measuring unit (16). A generation unit (111) generates a key based on the quantities of each component which is acquired with the acquisition unit (115). An encryption unit (112) encrypts data using the key which is generated with the generation unit (111) and generates encrypted data. A communication unit (13) transmits the encrypted data which is generated by the encryption unit (112) to a receiving-side information transmission terminal (1).

(57) 要約: 【課題】暗号通信に用いる鍵を予測され難くする。【解決手段】送信側の情報伝送端末 1 において、測定部 16 は、試料に含まれる複数の成分の量をそれぞれ測定する。取得部 115 は、測定部 16 により測定された成分の量を示す情報を取得する。生成部 111 は、取得部 115

により取得された各成分の量に基づいて鍵を生成する。暗号化部 112 は、生成部 111 により生成された鍵を用いてデータを暗号化して暗号データを生成する。通信部 13 は、暗号化部 112 により生成された暗号データを受信側の情報伝送端末 1 へ送信する。

明 細 書

発明の名称： 情報伝送端末

技術分野

[0001] 本発明は、情報伝送端末による暗号通信に関するものである。

背景技術

[0002] 情報を保全する目的でパスワードやパスフレーズなどが鍵として採用されることがある。安全性の面からこの鍵には複雑な文字列などが適しているが、鍵にあまり複雑なものを採用するとユーザが覚えられないことがある。一方、ユーザにとって覚えやすいものを鍵として採用すると、その鍵が不正利用者に推測されてしまう可能性がある。

[0003] そこで、物質の解析結果を情報の保全に利用することが考えられている。特許文献1には、複雑であり、無秩序であって、固有であり、且つ安定した構造を具備する材料要素の少なくとも1つの構造的な特性から得られた1つ又はいくつかのデジタル署名の使用法と、このような保護されたデータの媒体、並びに、この保護されたデータを読み取る方法が開示されている。特許文献2には、メモリタグを用いてランダムな特徴を有する物理オブジェクトの認証を行うことが開示されている。特許文献3には、化学元素の割合の分析ができるようにコーティング用組成物または印刷用インク中の適所に保持される無機粒子を標識付け手段として使用することが開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特表2007-520962号公報

特許文献2：特開2005-327248号公報

特許文献3：特表2002-500244号公報

発明の概要

発明が解決しようとする課題

[0005] しかしながら、特許文献1に開示された技術において、材料要素は、複雑

であり、無秩序であって、固有であり、且つ安定した構造を具備する必要があった。特に特許文献１に記載の技術は、材料要素の固有な構造を用いるので、その材料要素の代替物や複製物を使わず送受信の双方で共通の鍵を用いる暗号通信に利用することは困難であった。また、特許文献２に開示された技術は、基本媒体の特定位置の測定結果と予め記憶されている測定結果とが一致するか否かをチェックすることにより、基本媒体がオリジナルであるか否かをチェックするものであり、暗号通信に適用することが困難であった。また、特許文献３に開示された技術は、無機粒子を標識付手段として使用するものであって、偽造や無許可取引などを防止するために適用され得るが、メッセージを暗号化して通信に用いる暗号通信に利用することは困難であった。

[0006] 本発明は、暗号通信に用いる鍵を予測され難くすることを目的とする。

課題を解決するための手段

[0007] 本発明に係る情報伝送端末は、一の態様において、試料に含まれる一以上の成分についての情報を取得する取得部と、前記取得部により取得された前記情報に基づいて鍵を生成する生成部と、前記生成部により生成された鍵を用いてデータを暗号化して暗号データを生成する暗号化部と、前記暗号化部により生成された暗号データを他の情報伝送端末へ送信する送信部とを具備する。

[0008] 本発明に係る情報伝送端末は、他の態様において、他の情報伝送端末から暗号データを受信する受信部と、試料に含まれる一以上の成分についての情報を取得する取得部と、前記取得部により取得された前記各情報に基づいて鍵を生成する生成部と、前記受信部により受信された暗号データを、前記生成部により生成された鍵を用いて復号する復号部とを具備する。

[0009] 好ましくは、鍵を成分の量または物性を示す情報に基づいて生成する方法を特定する特定部を具備し、前記生成部は、前記特定部が特定した方法にしたがって、前記鍵を生成するとよい。

[0010] また、好ましくは、試料に含まれる一以上の成分についての情報を取得す

る方法を特定する特定部を具備し、前記取得部は、前記特定部が特定した方法にしたがって、前記各情報を取得するとよい。

[0011] また、好ましくは、暗号化の方法を特定する特定部を具備し、前記暗号化部は、前記特定部が特定した方法にしたがって、前記データを暗号化するとよい。

[0012] また、好ましくは、復号の方法を特定する特定部を具備し、前記復号部は、前記特定部が特定した方法にしたがって、前記暗号データを復号するとよい。

[0013] また、好ましくは、複数の選択肢をそれぞれ割り当てられた複数の項目に対してユーザがそれぞれ1つの選択肢を選択する操作を受け付ける操作部を具備し、前記特定部は、前記操作部が受け付けた操作が示す選択肢の組み合わせに応じて、前記方法を特定するとよい。

[0014] また、好ましくは、時刻を示す時刻情報を取得する時刻情報取得部を具備し、前記特定部は、前記時刻情報が示す時刻が含まれる期間に応じて、前記方法を特定するとよい。

[0015] 本発明の情報伝送方法は、一の態様において、送信装置に接続された測定部から、試料に含まれる一以上の成分についての情報を取得し、前記取得された情報に基づいて鍵を生成し、前記生成された鍵を用いてデータを暗号化して暗号データを生成し、前記生成された暗号データを送信することを特徴とする。

[0016] 本発明の情報伝送方法は、他の態様において、送信装置から暗号データを受信し、受信装置に接続された測定部から、試料に含まれる一以上の成分についての情報を取得し、前記取得された前記各情報に基づいて鍵を生成し、前記受信された暗号データを、前記生成された鍵を用いて復号する。

[0017] 本発明の情報伝送方法は、さらに他の態様において、送信装置と受信装置のそれぞれにおいて試料に含まれる複数の成分の量または物性の少なくとも1つを示す情報を取得し、前記取得された前記情報に基づいて暗号化鍵および復号化鍵をそれぞれ生成し、前記送信装置と前記受信装置との間の通信に

において、前記暗号化鍵を用いて暗号化されたデータの送信と、当該暗号化されたデータの前記復号化鍵を用いた復号とが実行される。

発明の効果

[0018] 本発明によれば、暗号通信に用いる鍵を予測され難くすることができる。

図面の簡単な説明

[0019] [図1]実施形態に係る通信システムの概要を示す図である。

[図2]情報伝送端末の構成を示す図である。

[図3]情報伝送端末の暗号化に係る機能的構成を示す図である。

[図4]情報伝送端末の復号に係る機能的構成を示す図である。

[図5]生成部が鍵を生成する動作の流れを示すフロー図である。

[図6]測定部により測定された試料の化学組成を表すグラフである。

[図7]測定部により測定された各成分のピーク値と量子化値を表す図である。

[図8]各成分の量子化値を配列した状態を示す図である。

[図9]変形例における情報伝送端末の暗号化に係る機能的構成を示す図である。
。

[図10]変形例における情報伝送端末の復号に係る機能的構成を示す図である。
。

[図11]測定対象となる成分の組み合わせを示す図である。

[図12]量子化法の種類を示す図である。

[図13]配列法の種類を示す図である。

[図14]測定方法の種類を示す図である。

[図15]変形例に係る通信システムの全体構成を示す図である。

[図16]変形例に係る情報伝送端末の構成を示す図である。

[図17]変形例に係る通信システムの構成を示す図である。

[図18]変形例に係る端末の機能構成を示す図である。

[図19]変形例に係る送信動作例を示す図である。

[図20]変形例に係る受信動作例を示す図である。

符号の説明

[0020] 1, 1 a…情報伝送端末、1 1…制御部、1 1 1…生成部、1 1 2…暗号化部、1 1 3…復号部、1 1 4…特定部、1 1 5…取得部、1 2…記憶部、1 3…通信部、1 4…操作部、1 5…表示部、1 6…測定部、1 6 a…インターフェース、1 7…收音部、1 8…放音部、2…通信網、3…測定装置、9, 9 a…通信システム

発明を実施するための形態

[0021] 1. 実施形態

1-1. システムの構成

図1は、実施形態に係る通信システム9の概要を示す図である。通信システム9は、複数の情報伝送端末1と、これらを互いに接続する通信網2とを有する。情報伝送端末1は、通信網2を介して通信を行う端末であり、本実施形態では電子メールの送受信を行う移動電話機である。通信網2は、情報伝送端末1同士を接続する通信網であり、本実施形態では移動体通信網である。情報伝送端末1の個数は2つに限らず3つ以上であってもよい。

[0022] 1-2. 情報伝送端末の構成

図2は、情報伝送端末1の構成を示す図である。制御部1 1は、CPU (Central Processing Unit)、ROM (Read Only Memory)、RAM (Random Access Memory) を備え、CPUが、ROMに記憶されているブートローダや記憶部1 2に記憶されているプログラムをRAMに読み出して実行することにより情報伝送端末1の各部を制御する。

[0023] 記憶部1 2はソリッドステートドライブやEEPROM (Electrically Erasable and Programmable Read Only Memory) などの記憶手段であり、制御部1 1に読み込まれるプログラムや各種データを記憶する。

通信部1 3は、通信網2と接続して通信を行う回路である。

操作部1 4は、各種の指示を入力するためのボタンやセンサなどの操作子を備えており、ユーザによる操作を受け付けてその操作内容に応じた信号を制御部1 1に供給する。

表示部1 5は、液晶を使用したディスプレイ装置であり、制御部1 1から

供給される信号に応じて画像を表示する。

[0024] 測定部 16 は、試料を受け入れてその試料の化学組成を測定する移動式の測定機器である。測定部 16 は、具体的には高速液体クロマトグラフィーを用いた有機酸の測定装置である。情報伝送端末 1 のユーザは、食品や飲料などの試料を決められた溶媒に決められた割合で溶解させて溶液を調整し、これをガラス容器などであるアンプル A m に封入する。測定部 16 は、多孔性固体などが充填されたカラムと、このカラムに通じたソケット S c を有している。ユーザにより上記のアンプル A m がこのソケット S c に挿し込まれると、測定部 16 のカラムは、アンプル A m に封入された上記の溶液を受け入れる。測定部 16 は、受け入れた試料に含まれる複数の成分の量を示す成分値をそれぞれ取得し、これら各成分値に応じた信号を制御部 11 に供給する。

[0025] ここでいう「成分値」とは、例えば試料が複数種類の物質からなる混合物の場合における各物質の存在割合（例えば重量濃度やモル濃度などによって表される）ものであってもよいし、試料が一の種類の化合物である場合にはその元素組成比であってもよいし、一つの成分が全体に占める割合であってもよい。

要は、試料を成分の観点から、何らかの方法で分析した結果得られる質量や比重などの物理量であればよい。

「液体クロマトグラフィー法」は、試料を液体化させて赤外線吸収量を測定するにより、複数の成分についての情報を一度に取得することが可能である。また、液体クロマトグラフィー法に替えて、ガス化した試料に対して計測を行うガスクロマトグラフィー法を用いてもよい。

ただし、測定部 16 の測定方法はクロマトグラフィー法等の、物質の分離を前提とした分析手法に限定されるものではなく、あらゆる分析手法を適用することが可能である。また、測定した情報のすべてを制御部 11 に供給する必要はなく一部のみを供給してもよい。例えば、試料中の複数の成分についての情報（成分比など）が測定された場合、一部の成分についての情報の

みを供給してもよい。なお、成分には、異物として認識される物質の成分も含む。また、一つの成分についての複数の情報（例えばpH（水素イオン濃度）と塩分（ナトリウム）濃度など）が測定された場合に、そのうちの一つの情報のみを供給してもよい。

具体的な測定装置の例としては、pHメータや塩分分析計、糖度分析計、導電率計、比抵抗計、TOC計、蛍光分光測定装置、ラマン分光測定装置、各種小型分析器やFTIR装置が挙げられ、本発明においては、これらのいずれも用いることができるが、これらは単に例示あって、これらに限定されるものではない。

[0026] 収音部17は、周囲の音声に応じた音声信号を発生させるマイクを有し、発生させた音声信号をデジタル信号に変換して制御部11に供給する。

放音部18は、音声を発生させるスピーカを有し、制御部11の制御の下、指示された音声信号をアナログ信号に変換してその信号に応じた音声をスピーカにより発生させる。

[0027] 1-3. 情報伝送端末の機能的構成

図3は、情報伝送端末1の暗号化に係る機能的構成を示す図である。情報伝送端末1の制御部11は、電子メールの送信に際し、図3に示す生成部111、暗号化部112および取得部115として機能する。取得部115は、使用する試料の各成分値に応じた信号（情報）を測定部16から取得する。生成部111は、これらの各信号、すなわち、取得部115により取得された各成分の量に基づいて鍵を生成する。この鍵とはデジタルデータで表される電子鍵である。

[0028] 暗号化部112はメッセージを暗号化する。メッセージとは、送信の対象となるデータであり、例えば人に伝える文書や音声、映像などを表したデータである。この例においてメッセージは、送信するために編集され記憶部12に記憶されている電子メールのデータである。暗号化部112は、記憶部12からメッセージを読み出し、決められた共通鍵暗号方式によって、生成部111により生成された鍵を用いて暗号化して暗号データを生成する。通

信部 1 3 は、暗号化部 1 1 2 により生成された暗号データを電子メールとして他の情報伝送端末 1 へ送信する。

[0029] 図 4 は、情報伝送端末 1 の復号に係る機能的構成を示す図である。情報伝送端末 1 の制御部 1 1 は、暗号化された電子メールの受信に際し、図 4 に示す生成部 1 1 1 および復号部 1 1 3 として機能する。電子メールの受信時における通信部 1 3 は、送信側の情報伝送端末 1 から電子メールとして暗号データを受信する。生成部 1 1 1 は、電子メール送信時と同様に測定部 1 6 から取得した各成分値に応じた信号に基づいて鍵を生成する。

[0030] 復号部 1 1 3 は暗号データを復号してメッセージにする。復号部 1 1 3 は、通信部 1 3 により受信された暗号データを、決められた共通鍵暗号方式によって、生成部 1 1 1 により生成された鍵を用いて復号してメッセージを生成する。生成されたメッセージは、記憶部 1 2 に記憶される。

[0031] 1-4. 鍵生成の動作

図 5 は、生成部 1 1 1 が鍵を生成する動作の流れを示すフロー図である。生成部 1 1 1 は、測定部 1 6 から各成分値に応じた信号を取得すると（ステップ S 1 0 1）、取得した各信号に基づいて、鍵の要素として用いるデジタル信号である量子化値を生成する量子化を行う（ステップ S 1 0 2）。

[0032] 図 6 は、測定部 1 6 により測定された試料のクロマトグラムである。図 6 の横軸は試料がカラムに投入されてからカラムを通過するまでの時間を示し、縦軸は、その時間にカラムを通過した成分の量を示す。試料に含まれている各成分は、それぞれカラムを通過する速度が異なるので、カラムを通過するまでの時間に差が生じる。カラムの後には電気伝導度測定器が備えられている。カラムを通過した溶液は、この電気伝導度測定器により電気伝導度を測定される。この電気伝導度は、溶液に含まれる成分の量と相関を有するので、上記の電気伝導度の時間変化を表すクロマトグラムにおいて、試料に含まれる各成分の量がピーク値として得られる。

[0033] 図 7 は、測定部 1 6 により測定された各成分のピーク値と量子化値を表す図である。図 6 に示した「8. 6 分」の位置には、成分番号「2」の成分の

ピークが現れる。このピークにおいて測定された電気伝導度に基づき、成分番号「2」の成分の量に応じた成分値として十進数表記で「9.5」という数値が得られる。この数値を示す信号を測定部16から取得すると、生成部111は、これに対し「切り捨て」という量子化を行う。その結果、生成部111は、上記の数値の小数点以下を切り捨て、十進数表記で「9.0」、二進数表記で「1001」という数値を示す量子化値を生成する。このようにして、図7に示すように、試料に含まれる成分番号「1」から「9」までの各成分に対して、鍵の要素として用いられる量子化値がそれぞれ生成される。なお、ここでいう量子化は、アナログ信号からデジタル信号を生成することに加え、デジタル信号からデジタル信号を生成することを含む。

[0034] 生成部111は、量子化により生成された量子化値を決められた規則に沿って配列し（ステップS103）、鍵に変換する（ステップS104）。

図8は、各成分の量子化値を配列した状態を示す図である。図7に示した各量子化値は、最上位桁を表す左端から成分番号の順に配列され、二進数表記で「11000100110011110111101001100」という数値となる。そして、この配列された二進数表記の数値の最下位側（右端）の4桁を十六進数表記における1の位の値とする「右詰め」がなされ、全体が1つの数値に変換される。図8に示す例においてこの数値は、十六進数表記で「1899EF4C」である。この数値が情報伝送端末1で電子メール送信時および受信時に、鍵として用いられる。なお、この鍵は一例であり、鍵の桁数はこれより多くても少なくてもよい。

[0035] 以上の動作によって得られた鍵により、送信側の情報伝送端末1は、メッセージとしての電子メールを暗号化した暗号データを送信する。受信側の情報伝送端末1は、送信側の情報伝送端末1で測定された試料と同種の試料を測定することで、送信側の情報伝送端末1で利用された鍵と同じ鍵を生成する。そして、受信側の情報伝送端末1は、この鍵を用いて受信した暗号データを復号してメッセージを生成する。その結果、この通信システム9によれば、送信側の情報伝送端末1のユーザと、受信側の情報伝送端末1のユーザ

との間で、共通の化学物質を試料として用いることを示し合わせておくことで暗号通信を行うことができる。

[0036] 2. 変形例

上記実施形態の内容は以下の観点から変形し得る。また、これらの観点を組み合わせてもよい。

2-1. 試料の内蔵

上述した実施形態において、測定部16は、試料を封入したアンプルAmを挿し込むソケットScを有していたが、測定部16は、試料そのものを予め内蔵していてもよい。この場合、内蔵された試料はユーザに対して秘匿されていてもよい。測定部16は、内蔵されたこの試料を構成する複数の成分の成分値をそれぞれ取得し、これら各成分値に応じた信号を制御部11に供給すればよい。各成分値に応じた信号に基づいて生成部111が生成した鍵は、暗号化および復号に用いられるほか、情報伝送端末1を識別する識別情報として用いられてもよい。

[0037] 2-2. 試料と鍵を生成する方法との組

上述した実施形態において、情報伝送端末1は、予め示し合わせた試料を送信側および受信側でそれぞれ用いることで暗号通信を行っていたが、この試料と、この試料から鍵を生成する方法との組によって決まる暗号通信を行ってもよい。

[0038] 図9は、この変形例における情報伝送端末1の暗号化に係る機能的構成を示す図である。また、図10は、この変形例における情報伝送端末1の復号に係る機能的構成を示す図である。特定部114は、ユーザの操作内容に応じた信号を操作部14から受け取ると、この信号に基づいて生成部111が鍵を生成する方法を決定して生成部111に伝える。

[0039] 例えば、図11は、測定対象となる成分の組み合わせを示す図である。図11において、セットA、セットB、セットCとは、測定対象となる成分の各組を互いに識別するための名称であり、各組ごとに、成分番号に対応付けて図6に示したカラムの通過時間（単位：分）が記述されている。例えば、

セットAにおいて、成分番号「1」は、カラムの通過時間が「8. 1分」の成分に割り当てられている。なお、使用しない成分番号には、通過時間を特定しないことを示す「-」が記述されている。制御部11は、図2に示す表示部15により、セットA、セットB、セットC…をそれぞれ選択肢としてユーザに表示させる。ユーザは操作部14を操作してセットA、セットB、セットC…のいずれかを選択する操作を行う。特定部114は、操作部14が受け付けたユーザの操作が示す選択肢により、測定対象となる成分の組を特定する。生成部111は、上述の特定された成分の組を測定対象とする方法により鍵を生成する。

[0040] また、図12は、量子化法の種類を示す図である。図12において、量子化法「 α 」「 β 」「 γ 」とは、それぞれ「切り捨て」「切り上げ」「2倍後四捨五入」に対応付けられている。例えば、制御部11は、表示部15により、量子化法 α 、量子化法 β 、量子化法 γ …をそれぞれ選択肢としてユーザに表示させる。ユーザは操作部14を操作して量子化法 α 、量子化法 β 、量子化法 γ …のいずれかを選択する操作を行う。特定部114は、操作部14が受け付けたユーザの操作が示す選択肢により、量子化法の種類を特定する。生成部111は、上述の特定された種類の量子化法を用いた方法により鍵を生成する。

[0041] ここでユーザが量子化法「 β 」を選択した場合、特定部114は、量子化法として「切り上げ」が選択されたことを生成部111に伝える。そして上述したように、或るピーク値として十進数表記で「9. 5」という数値が得られたとすると、生成部111は、これに対し「切り上げ」という量子化を行う。具体的には、生成部111は、上記のピーク値の小数点以下を切り上げ、十進数表記で「10. 0」、二進数表記で「1010」という量子化値を生成する。また、ユーザが量子化法「 γ 」を選択した場合、特定部114は、量子化法として「2倍後四捨五入」が選択されたことを生成部111に伝える。このとき、生成部111は、十進数表記で「9. 6」というピーク値を得た場合に、これを2倍して十進数表記で「19. 2」にし、小数点以

下を四捨五入する。その結果、生成部 111 は、十進数表記で「19.0」、二進数表記で「10011」という量子化値を生成する。

[0042] また、図 13 は、配列法の種類を示す図である。制御部 11 は、表示部 15 により、配列法 I、配列法 II、配列法 III…をそれぞれ選択肢としてユーザに表示させる。ユーザは操作部 14 を操作して配列法 I、配列法 II、配列法 III…のいずれかを選択する操作を行う。特定部 114 は、操作部 14 が受け付けたユーザの操作が示す選択肢により、配列法の種類を特定する。生成部 111 は、上述の特定された配列法により鍵を生成する。

[0043] 図 13 において、配列法 I は「左詰」であり、各成分の量子化値を最上位桁である左端から詰めていき、左端から順に変換する方法である。配列法 I が選択されたとき、生成部 111 は、二進数表記した量子化値を並べ、左端から 4 桁ずつを 1 桁の 16 進数に変換する。そして、右端に残った数値が 4 桁に満たない場合、生成部 111 は、この残った数値の右側に二進数表記の「0」を詰めて 4 桁にしてこれを 1 桁の 16 進数に変換する。これによれば、図 8 に示した二進数表記の数値は、右端に二進数表記における「0」が 3 桁詰められた上で、十六進数表記で「C4CF7A60」に変換される。

[0044] 配列法 II は「右詰」であり、上述したように二進数表記の数値の最下位側の 4 桁を 1 の位として、変換を行う方法である。配列法 III は「パディング」であり、各成分の量子化値にそれぞれ決められた桁数を確保して、量子化値を表さないビットにパッドとして 0 を詰め込む方法である。配列法 III が選択されたとき、生成部 111 は、例えば、全ての量子化値に二進数表記で 5 桁をそれぞれ確保する場合、二進数表記で「11000・1001・100・111・101・11・10・1001・100」という上述した数値ではなく、「11000・01001・00100・00111・00101・00011・00010・01001・00100」という数値を得る。なお、ここで中点「・」は、各成分の区切りを示すための記号である。

[0045] 以上のように、測定部 16 により測定される試料が同じであっても、鍵を

生成する方法が異なることにより異なる鍵が生成される。したがって、電子メールの送信者および受信者は、試料と、この試料から鍵を生成する方法との「組」を示し合わせ、これによって電子メールを情報伝送端末１に暗号化および復号させて暗号通信を行えばよい。なお上述した例では、測定対象となる成分の組み合わせ、量子化法、および配列法という複数の項目についてそれぞれ複数の選択肢が割り当てられており、ユーザは、各項目に対して１つの選択肢を選択していた。すなわち、鍵を生成する方法は、ユーザの選択した選択肢の組み合わせによって特定されてもよい。例えば、鍵を生成する方法が、複数の工程に分解されるといった場合に、情報伝送端末１は、各工程を示す項目ごとに選択肢を表示してユーザに選択させる。そして、情報伝送端末１は、選択された各選択肢の組み合わせによってこの「鍵を生成する方法」を特定すればよい。

また、上記例示した複数の測定方法を二以上用いてもよい。この場合、それぞれの測定方法にて得られる結果（成分値もしくは物性値等）の任意の組み合わせで鍵の生成に利用してもよい。勿論、一の測定方法において複数の成分値もしくは物性値が得られる場合は、それらを任意の組み合わせで利用してもよい。

[0046] ２－３．試料と、成分の量を取得する方法との組

上記の変形例では、試料と組み合わせる情報として、測定対象となる成分の組み合わせ、量子化法、および配列法という、「鍵を生成する方法」の構成要素を挙げたが、他の処理に関する情報と組み合わせてもよい。例えば、成分の量を取得する方法のうち、例えば、測定方法を示す情報であってもよい。図１４は、測定方法の種類を示す図である。図１４において、測定法Ａは「ガスクロマトグラフィー」であり、測定法イは「液体クロマトグラフィー」であり、測定法ウは「赤外分光測定」である。

[0047] 例えば、情報伝送端末１には測定方法の異なる複数の測定部１６が設けられていて、図１４に示すいずれかの測定法がユーザにより操作部１４を介して選択されたとき、特定部１１４は、図９および図１０に破線で示すように

、選択された測定方法を取得部 115 に伝える。取得部 115 は、この測定方法に応じて、複数の測定部 16の中から使用する測定部 16を決定する。これにより、同じ試料を用いても測定方法が異なるために生成される鍵は異なったものとなる。なお、上記の測定方法は、複数の項目について選択された選択肢の組み合わせによって特定されてもよい。

[0048] 2-4. 試料と暗号化・復号の方法との組

また、試料と組み合わせる情報として、暗号化または復号の方法を示す情報が用いられてもよい。暗号化または復号の方法とは、それらに用いられるアルゴリズムなどであり、例えば、DES (Data Encryption Standard) や AES (Advanced Encryption Standard) などである。これらアルゴリズムの種類をユーザに選択させ、生成部 111 は、選択されたアルゴリズムにしたがって暗号化および復号を行うようにすればよい。この場合、特定部 114 は、図 9 および図 10 に破線で示すように、選択されたアルゴリズムを利用する旨を暗号化部 112 や復号部 113 に伝えればよい。

なお、上記の暗号化または復号の方法は、複数の項目について選択された選択肢の組み合わせとして特定されてもよい。

[0049] 2-5. インターフェース

上述した情報伝送端末 1 は測定部 16 を備えていたが、これに代えて外部の測定装置と接続してその測定装置から測定結果を取得するインターフェースを備えていてもよい。図 15 は、この変形例に係る通信システム 9a の全体構成を示す図である。通信システム 9a は、情報伝送端末 1a が測定装置 3 と接続するように構成されている点が上述した実施形態に係る通信システム 9 と異なっている。

[0050] 図 16 は、情報伝送端末 1a の構成を示す図である。情報伝送端末 1a は、測定部 16 に代えて外部の測定装置 3 と接続するインターフェース 16a を備えている点が、実施形態に係る情報伝送端末 1 と異なっている。制御部 11 は、インターフェース 16a を介して測定装置 3 から、試料に含まれる複数の成分の量をそれぞれ取得すればよい。このようにインターフェース 1

6 aを介して測定装置3に接続することで、情報伝送端末1 aは測定のための構成を内蔵する必要がなくなるので、軽量化が図れ、携帯電話機など携帯に適したものとすることができる。また、この場合の測定装置3は固定されていてもよい。

[0051] 2-6. プログラム

情報伝送端末1 (1 a)の制御部11によって実行される各プログラムは、磁気テープや磁気ディスクなどの磁気記録媒体、光ディスクなどの光記録媒体、光磁気記録媒体、半導体メモリなどの、コンピュータ装置が読み取り可能な記録媒体に記憶された状態で提供し得る。また、このプログラムを、インターネットなどのネットワーク経由でダウンロードさせることも可能である。なお、上記の制御部11によって例示した制御手段としてはCPU以外にも種々の装置が適用される場合があり、例えば、専用のプロセッサなどが用いられる。

[0052] 2-7. 暗号化の対象

上述した実施形態において、暗号化される対象である「メッセージ」は電子メールなどのデータであったが、通話音声を示す音声データやストリーミング映像を示す映像データなどであってもよい。また、暗号化される対象は人間に理解得る情報でなくてもよい。例えば、他の暗号化処理によって暗号化されたデータであってもよい。この場合、情報伝送端末1は、この暗号化されたデータをさらに暗号化して他の情報伝送端末1へ送信すればよい。要するにメッセージは送信の対象となるデータであればよい。

[0053] 2-8. 測定項目

上述した実施形態において、測定部16により測定される項目は試料の各成分の量を示す成分値であったが、これに加えて、またはこれに代えて、試料の物理的特性(物性)が測定されてもよい。物性とは、その物質に固有な巨視的な力学的・熱的・電氣的・磁氣的・光学的などの性質であって、例えば光透過率や屈折率、反射率、透磁率、熱伝導率、電気伝導率などによって評価される。好ましい態様において、これらの物性パラメータの少なくとも

いずれか一つと、決められた少なくとも一つ以上の成分の値とに基づいて、生成部 1 1 1 が鍵を生成すればよい。

本発明の情報伝送端末は、一の態様において、試料に含まれる一以上の成分についての情報を取得する取得部と、前記取得部により取得された前記情報に基づいて鍵を生成する生成部を有し、且つ前記生成部により生成された鍵を用いてデータを暗号化して暗号データを生成して他の情報伝送端末へ送信する送信部と、他の情報伝送端末から暗号データを受信して前記生成部により生成された鍵を用いて復号する受信部の少なくともいずれかを有していればよい。

試料に含まれる一以上の成分についての情報とは、所定の 1 以上の成分が全体に占める割合（重量比や体積比とうの成分比）あるいは一以上の成分の各々についての物理的特性を表わす量であり、さらに一の成分についての成分比と物理量とを組み合わせたものであってもよい。

本発明の情報伝送方法は、一の態様において、送信装置と受信装置のそれぞれにおいて用意された試料に含まれる、(a) 少なくとも 1 つの成分の量を示す情報および (b) 当該試料の物性を表わす少なくとも 1 つの情報のうち、少なくともいずれか一方の情報を取得し、前記取得された前記情報に基づいて暗号化鍵および復号化鍵を生成し、前記送信装置と前記受信装置との間の通信において、前記暗号化鍵によって暗号化されたデータの送信と、当該暗号化されたデータの前記復号化鍵を用いた復号が実行される。

[0054] 2-9. 検出

上述した実施形態において、測定部 1 6 は、各成分値を測定していたが、測定部 1 6 に代えて、その成分の有無を検出する検出部（または検出装置）を用いてもよい。この検出部は各成分を定性的に検出すればよく、各成分の量を定量しなくてもよい。また、各成分値を測定して、その測定値と予め決められている閾値とを比較し、各成分の有無を検出してもよい。生成部 1 1 1 は、例えば、検出された成分に数値「1」を、検出されなかった成分に数値「0」を割り当てて、決められた順序でこれらの数値を配列する。このよ

うにして配列された数値は二進数となっているので、生成部 111 はこれに基づいて鍵を生成すればよい。

[0055] 2-10. 時系列変化

上述した実施形態において、鍵を生成する方法、測定方法、暗号化または復号の方法は予め決められたものであった。また、上述した変形例において、これらの方法は、ユーザの操作に応じて決められるものであった。しかし、これらの方法を決めるのはユーザの操作に限られない。例えば、これらの方法は、時刻に応じて決められてもよい。以下に、この態様に含まれる例を示す。

[0056] (1) スケジュール

情報伝送端末 1 の記憶部 12 には、予め上記の方法について複数の種類を定め、これらが毎日変化するように設定されたスケジュールが記憶されている。

まず、送信側の情報伝送端末 1 の制御部 11 は、内蔵されたタイマを参照して現在の時刻を示す時刻情報を取得する。そして、制御部 11 は、上記のスケジュールを参照して、この時刻情報が示す時刻を含む今日の日付に対応付けられた測定方法を特定し、この測定方法に従って、試料に含まれる複数の成分の量を取得する。

次に、この制御部 11 は、上記のスケジュールを参照して、今日の日付に対応付けられた鍵の生成方法を特定し、この生成方法に従って、取得した成分の量から鍵を生成する。

その後、この制御部 11 は、上記のスケジュールを参照して、今日の日付に対応付けられた暗号化の方法を特定し、この暗号化の方法に従って、メッセージを暗号化し、得られた暗号データに今日の日付を付加して送信する。

受信側の情報伝送端末 1 は、暗号化の日付に対応する測定方法、鍵の生成方法、および復号の方法を記憶部 12 に記憶された上記のスケジュールからそれぞれ特定し、これらに従って、試料を測定し、鍵を生成して、暗号データを復号すればよい。

[0057] この変形例では、測定方法、鍵の生成方法、および暗号化・復号の方法が毎日変化するが、この変化の規則は送信側および受信側のそれぞれのユーザしか知らない。したがって、暗号に用いる際の試料を予め知らされていない上に、上記の変化の規則を知らない不正利用者にとっては暗号データの解読の困難性がさらに増すこととなる。なお、方法に対応付けられる期間は1日に限られず、他の期間（1週間など）であってもよい。各方法に異なる長さの期間が対応付けられていてもよい。

[0058] （2）周期

方法が周期的に変化する場合には、その1周期が定められていればよい。例えば、2つの方法を周期的に切り替えて用いる場合、日付が奇数日のときは第1の方法、偶数日のときは第2の方法を採用するように決めておいてもよい。

[0059] （3）演算

測定部16により得られる成分値や物性値など、鍵の生成に用いられる各種測定値に、時刻を示す数値を用いた演算を施してもよい。例えば、測定部16による測定結果に、その測定が行われた時刻を表す数値を乗算して、得られた数値に基づいて鍵を生成してもよい。この場合、生成された鍵を使って暗号化された暗号データに、この時刻を表す数値を付加して送信すればよい。鍵を生成する際の演算（この場合は、乗算）が秘匿されているため、不正利用者が暗号データに付加された数値を使って暗号を解読することは困難である。なお、この演算は複数の関数を組み合わせたものであってもよい。

[0060] 2-11. 情報伝送端末

上述の実施形態において、情報伝送端末1は、通信網2を介して他の情報伝送端末1と通信を行う移動電話機であったが、携帯電話機、PDA（Personal Digital Assistant）、携帯音楽再生機、携帯動画再生機、ゲーム機、電子書籍の閲覧装置、ナビゲーション装置、パーソナルコンピュータ等であってもよい。

[0061] 2-12. 具体的な変形例の一例

図17は、本発明の一実施例に係る通信システム100を示す。通信システム100は、端末100Aと端末100Bとを有する。端末100Aと端末100Bとはインターネット400を介してデータの送受信を行う。端末100A（100B）は一般的なパーソナルコンピュータとしての機能を備える。各端末100には測定装置200（200A、200B）とがUSB等のバスによって接続されている。

各測定装置200は、各端末100から出力された命令に応じて、試料が入った容器300（300A、300B）がセットされた場合に、当該試料の分析を行い、分析結果を各端末100に出力する。

暗号化通信を行う場合は、端末100Aのユーザと100Bのユーザとの間で、暗号化／復号に用いる試料の種類を事前に申し合わせておいてもよいし、暗号化データを送信する際に、試料の種類を指定する情報を暗号化されていない状態で相手に送信してもよい。

[0062] 図18に端末100の機能構成を示す。端末100は、制御部110と記憶部130と入力部150と通信部160とを含む。

[0063] 記憶部130は、送信すべきデータや受信したデータに加え、アルゴリズム生成情報を記憶する。アルゴリズム生成情報とは、試料の分析結果から暗号鍵をどのように生成するかを定義した情報である。例えば、分析結果に、複数の化合物の種類と各化合物の成分量（成分比）といった複数のパラメータが含まれる場合に、これらのパラメータのうちどれをどのように用いて暗号鍵を生成するのかを定義する情報である。あるいは、例えば、「成分比の高いものから3番目までの重量パーセント値を使用しこれらの3つの値を乗算する」することが定義される。

あるいは、分析結果が一つの値（たとえばpH濃度や塩分濃度）のみ含まれる場合において、その値をどのように加工して鍵を生成するのかを定義する情報であってもよい。例えば、分析装置からpH（水素イオン濃度）の測定結果として「5.04」という値を取得した場合に、この値と所定の他の情報（測定日時などの測定に付随する情報や測定温度などの測定条件・測定

環境に関する情報など）とを組み合わせで鍵を生成することを定義することができる。アルゴリズム生成情報は、暗号化通信を行う前に送信者と受信者との間で予め取り決めておく。また、アルゴリズム生成情報に、用いるべき試料の種類を含ませてもよい。

なお、分析結果の値を加工せずにそのまま使用するという情報をアルゴリズム生成情報に包含させてもよい。

すなわち、各端末１００において、暗号化通信を行う相手に関し、送信データの暗号化および受信データの復号に際して生成される鍵が一意に定まるように、少なくとも試料の種類が特定さればよく、加えて分析結果から鍵を用いる方法を特定してもよい。

[0064] 制御部１００は、ＣＰＵ等のプロセッサによって実現され、鍵生成部１１１、取得部１１２、暗号／復号処理部１１３およびアルゴリズム１２０を含む。

取得部１１２は、分析装置２００に分析の実行命令を出力し、分析装置２００から分析結果を取得して鍵生成部１１１に出力する。鍵生成部１１１は、取得部１１２から取得して分析結果とアルゴリズム特定部１２０から取得してアルゴリズム生成情報とに基づいて暗号化および復号に必要な鍵を生成し、暗号／復号処理部１１３に出力する。鍵とはは、例えば所定桁の数字の羅列である。暗号／復号処理部１１３は、所定のアルゴリズム（ＡＥＳ等）に従い、鍵生成部１１１から供給された鍵を用いて、送信データを暗号化して通信部１６０に出力する。また、通信部１６０から提供された受信データに、所定のアルゴリズム（ＡＥＳ等）に従い、鍵生成部１１１から供給された鍵を用いて復号し、表示部１４０および記憶部１３０に出力する。

アルゴリズム特定部１２０は、記憶部１３０からアルゴリズム生成情報を読み出して、鍵生成部１１１に出力する。

表示部１４０は液晶ディスプレイ等の表示装置である。通信部１６０は、通信処理プロセッサとして実現され、制御部１１０から出力されたデータを送信し、受信したデータを制御部１００に出力する。入力部１５０は、キー

ボードやマウス等のユーザによって操作される入力デバイスであって、制御部100への命令の入力や記憶部へのデータの格納等を行う。

[0065] 図19は、データを送信する際の動作の例を表わす図である。この例では、測定装置200Aおよび200BはpH測定計であり、端末100Aにおいては、アルゴリズム生成方法として、端末100Bと対応付けて、試料として飲料Y、および「測定値と測定した日時情報とをアルゴリズムAに従って演算する」という情報（これを情報Xとする）が記憶されているとする。そして端末100Bにおいては、当該情報Xが端末100Aに対応付け記憶されている。いま、端末100Aから端末100Bにデータを送信する場合を説明する。

[0066] 端末100Aのユーザは、通信相手（端末100B）と送信したいデータを指定する（S100）。続いて、端末100Bに対応する鍵生成アルゴリズム（情報X）を決定する（S102）。なお、相手ごとに異なる試料を使用することになっている場合は、その相手に対応した試料が少なくとも特定される。これに加えて、当該通信相手に対応付けて記憶部130に記憶された鍵生成アルゴリズムが読み出されてもよい。そして、ユーザはその試料（ここでは飲料Y）を分析装置200にセットし、所定の操作を行うと、試料の分析が行われる（S104）。分析結果が取得されると、分析結果であるpH値と情報Xとに基づいて鍵が生成される（S106）。生成された鍵を用いて当該データが暗号化され（S108）、当該通信相手に暗号化されたデータが送信される（S110）。なお、データの送信元の情報については平文であるとする。

[0067] 図20はデータを受信する際の動作の例を表わす図である。端末100Bは、暗号化されたデータを受信する（S200）。データの送信元が端末100Aであることを確認すると、用いるべき試料として飲料Yであることを含む情報Xを特定する（S202）。端末100Bのユーザは飲料Yをセットし、試料の分析命令を入力する（S204）。すると、鍵が生成され（S206）、この鍵を用いて受信したデータが復号され（S208）、復号後

のデータが表示部に表示されるとともに記憶部 130 に記憶される (S200)。

この例においては、pHを測定する装置を通信相手同士が所有していればよいので、クロマトグラフィー等の高性能だが高価な装置を用いなくても、物質の成分に基づいた情報によって鍵が生成されるので、手軽かつセキュリティの高い暗号化通信が実現される。

請求の範囲

- [請求項1] 試料に含まれる一以上の成分についての情報を取得する取得部と、
前記取得部により取得された前記情報に基づいて鍵を生成する生成部と、
前記生成部により生成された鍵を用いてデータを暗号化して暗号データを生成する暗号化部と、
前記暗号化部により生成された暗号データを送信する送信部とを具備する情報伝送端末。
- [請求項2] 暗号データを受信する受信部と、
試料に含まれる一以上の成分についての情報を取得する取得部と、
前記取得部により取得された前記情報に基づいて鍵を生成する生成部と、
前記受信部により受信された暗号データを、前記生成部により生成された鍵を用いて復号する復号部とを具備する情報伝送端末。
- [請求項3] 前記鍵を前記情報に基づいて生成する方法を特定する特定部を具備し、
前記生成部は、前記特定部が特定した方法にしたがって、前記鍵を生成することを特徴とする請求項 1 または 2 に記載の情報伝送端末。
- [請求項4] 前記情報を取得する方法を特定する特定部を具備し、
前記取得部は、前記特定部が特定した方法にしたがって、前記各情報を取得することを特徴とする請求項 1 または 2 に記載の情報伝送端末。
- [請求項5] 暗号化の方法を特定する特定部を具備し、
前記暗号化部は、前記特定部が特定した方法にしたがって、前記デ

ータを暗号化する

ことを特徴とする請求項 1 に記載の情報伝送端末。

[請求項6]

復号の方法を特定する特定部

を具備し、

前記復号部は、前記特定部が特定した方法にしたがって、前記暗号データを復号する

ことを特徴とする請求項 2 に記載の情報伝送端末。

[請求項7]

複数の選択肢をそれぞれ割り当てられた複数の項目に対してユーザがそれぞれ 1 つの選択肢を選択する操作を受け付ける操作部

を具備し、

前記特定部は、前記操作部が受け付けた操作が示す選択肢の組み合わせに応じて、前記方法を特定する

ことを特徴とする請求項 3 から 6 のいずれか 1 項に記載の情報伝送端末。

[請求項8]

時刻を示す時刻情報を取得する時刻情報取得部

を具備し、

前記特定部は、前記時刻情報が示す時刻が含まれる期間に応じて、前記方法を特定する

ことを特徴とする請求項 3 から 6 のいずれか 1 項に記載の情報伝送端末。

[請求項9]

送信装置に接続された測定部から、試料に含まれる一以上の成分についての情報を取得し、

前記取得された情報に基づいて鍵を生成し、

前記生成された鍵を用いてデータを暗号化して暗号データを生成し

、

前記生成された暗号データを送信する情報伝送方法。

[請求項10]

送信装置から暗号データを受信し、

受信装置に接続された測定部から、試料に含まれる一以上の成分に

ついでに情報を取得し、

前記取得された前記各情報に基づいて鍵を生成し、

前記受信された暗号データを、前記生成された鍵を用いて復号する
情報伝送方法。

[請求項11] 前記鍵を前記情報に基づいて生成する方法を特定し、
前記特定した方法にしたがって、前記鍵を生成することを特徴とする
請求項9または10に記載の情報伝送方法。

[請求項12] 前記情報を取得する方法を特定し、
前記特定した方法にしたがって、前記各情報を取得することを特徴
とする請求項9または10に記載の情報伝送方法。

[請求項13] 前記取得した情報に基づき暗号化の方法を特定し、
前記特定した方法にしたがって、前記データを暗号化することを特
徴とする請求項9に記載の情報伝送方法。

[請求項14] 前記取得した情報に基づき復号の方法を特定し、
前記特定した方法にしたがって、前記暗号データを復号することを
特徴とする請求項10に記載の情報伝送方法。

[請求項15] 複数の選択肢をそれぞれ割り当てられた複数の項目に対してユーザ
がそれぞれ1つの選択肢を選択する操作を受け付け、
前記受け付けた操作が示す選択肢の組み合わせに応じて、前記方法
を特定することを特徴とする請求項11から14のいずれか1項に記
載の情報伝送方法。

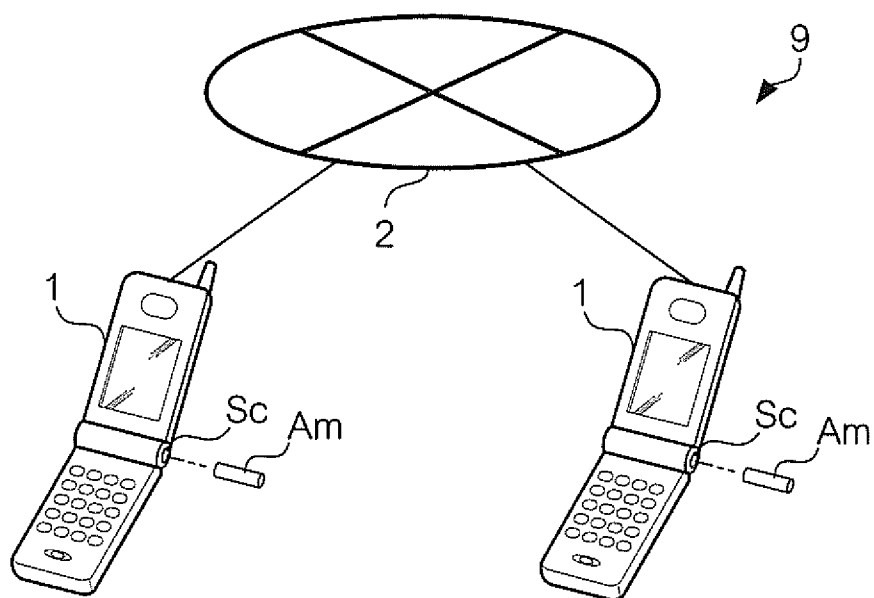
[請求項16] 時刻を示す時刻情報を取得し、
前記特定部は、前記時刻情報が示す時刻が含まれる期間に応じて、
前記方法を特定することを特徴とする請求項11から14のいずれか
1項に記載の情報伝送方法。

[請求項17] 送信装置と受信装置のそれぞれにおいて試料に含まれる一以上の成
分についての情報を取得し、
前記取得された前記情報に基づいて暗号化鍵および復号化鍵をそれ

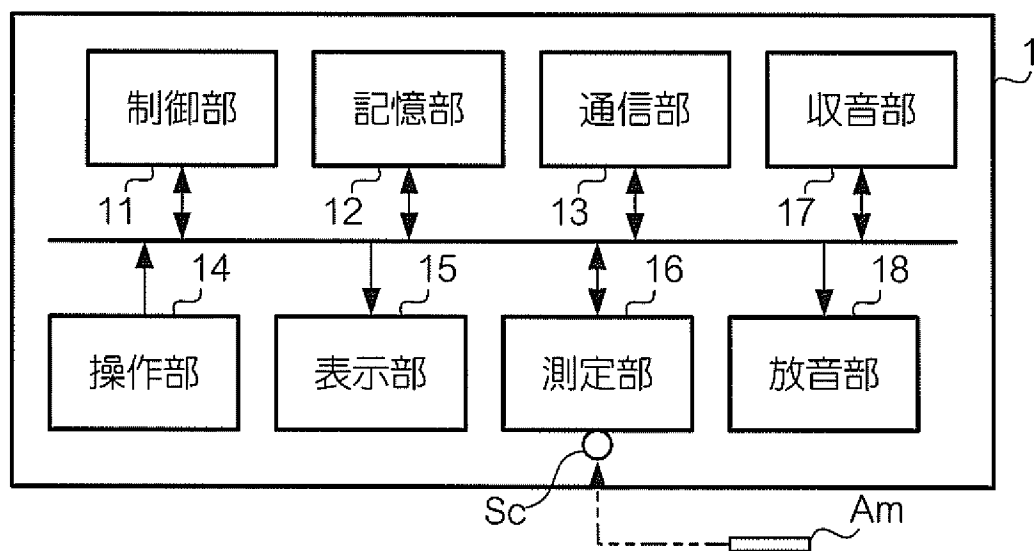
ぞれ生成し、

前記送信装置と前記受信装置との間の通信において、前記暗号化鍵を用いて暗号化されたデータの送信と、当該暗号化されたデータの前記復号化鍵を用いた復号とが実行されることを特徴とする情報伝送方法。

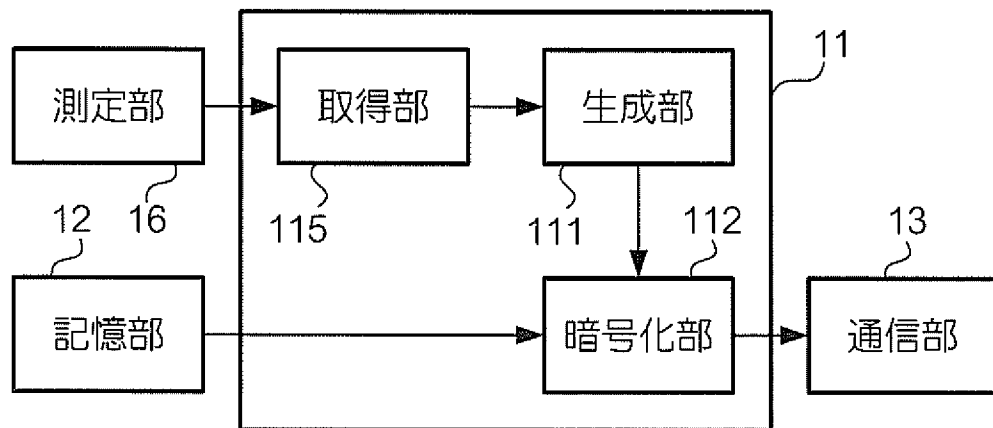
[図1]



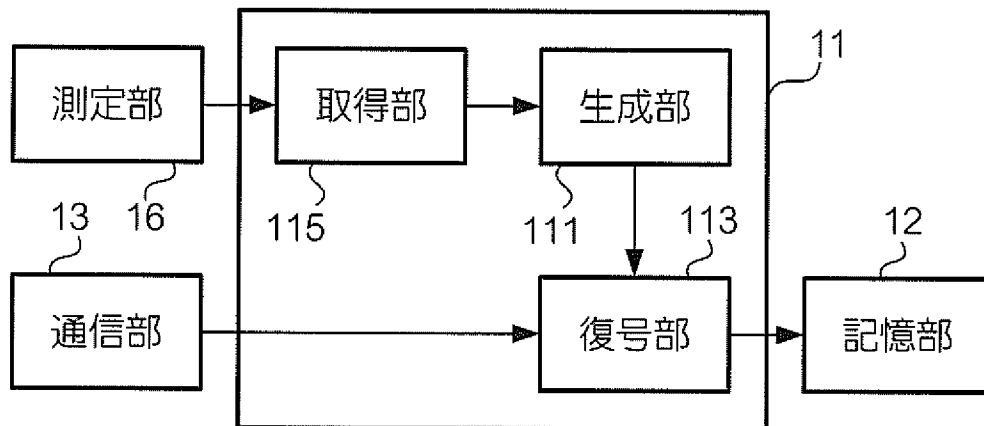
[図2]



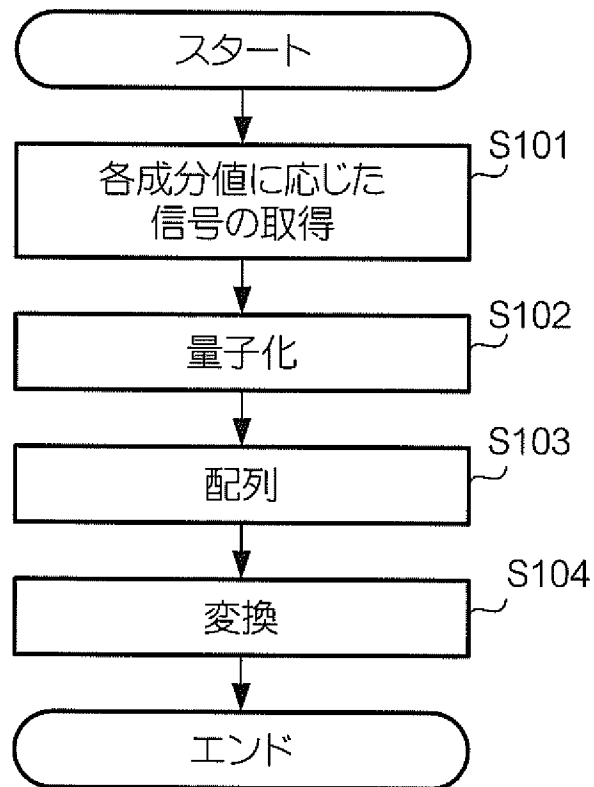
[図3]



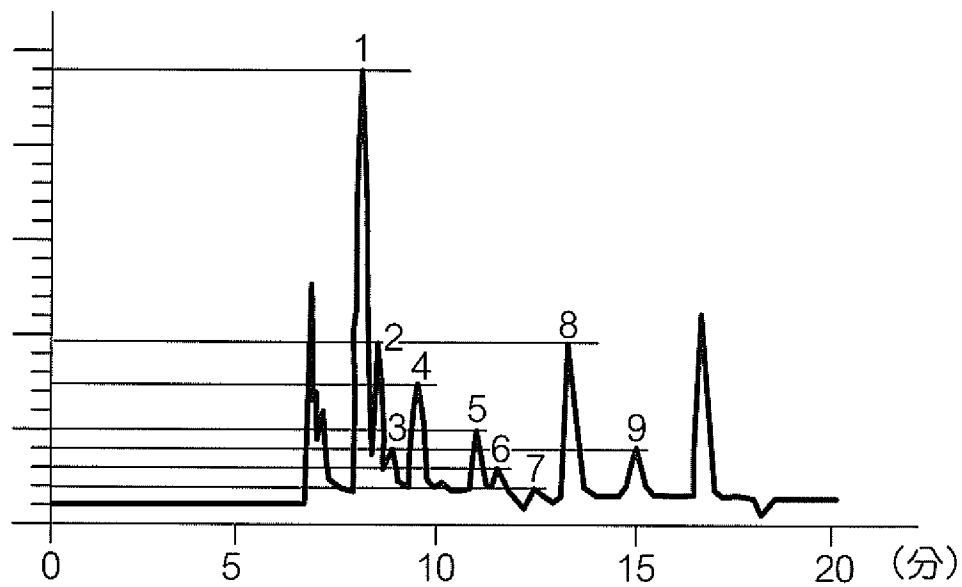
[図4]



[図5]



[図6]

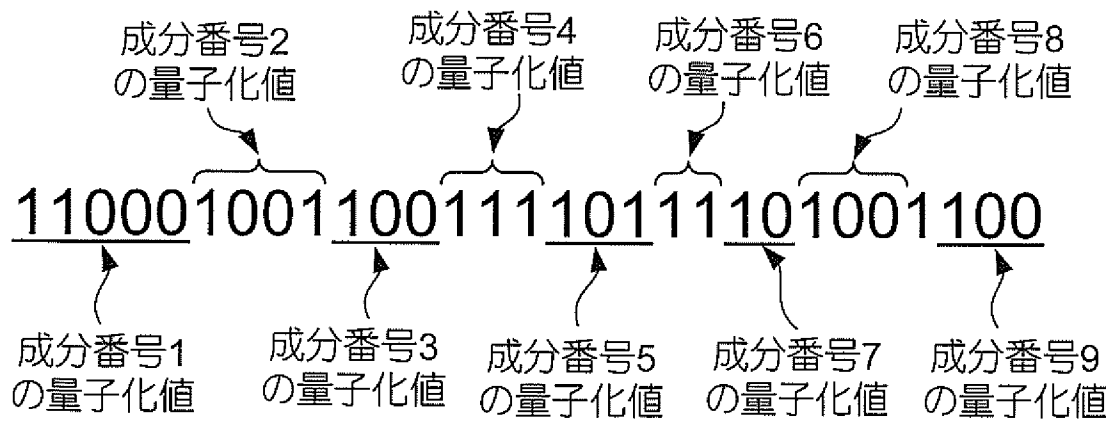


[図7]

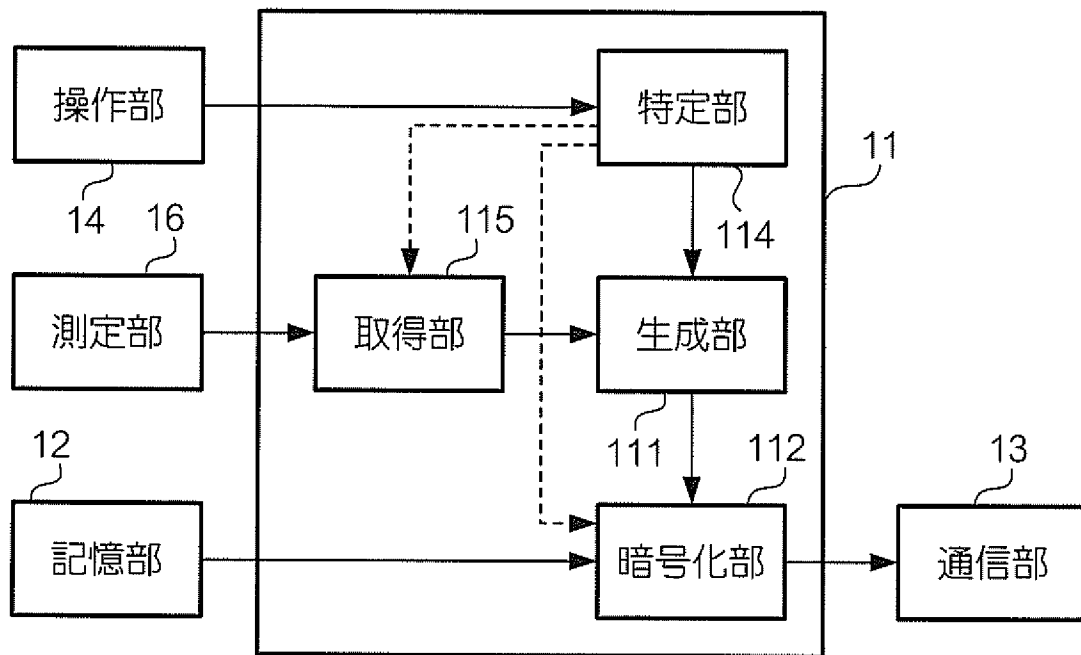
成分番号	1	2	3	4	5
ピーク値	24.0	9.5	4.0	7.5	5.0
量子化値	11000	1001	100	111	101

成分番号	6	7	8	9
ピーク値	3.0	2.0	9.5	4.0
量子化値	11	10	1001	100

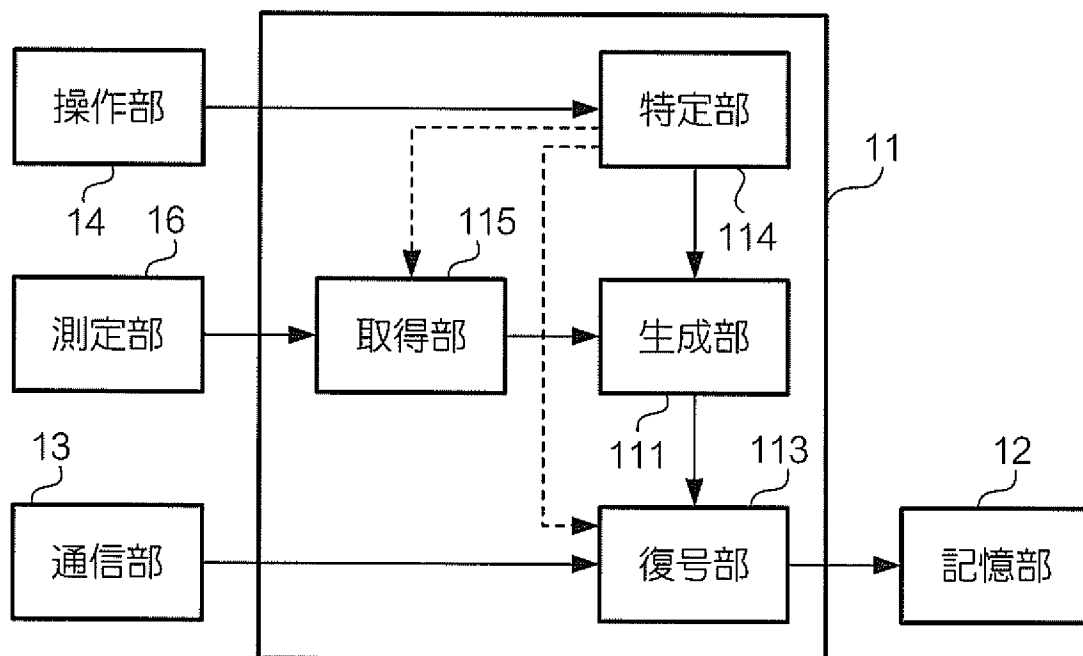
[図8]



[図9]



[図10]



[図11]

成分番号	1	2	3	4	5	6	7	8	9
セットA	8.1	8.6	8.9	9.5	10.9	11.5	12.3	13.4	14.9
セットB	14.9	13.4	12.3	11.5	10.9	9.5	8.9	8.6	8.1
セットC	8.1	11.5	10.9	12.3	14.9	8.6	—	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

[図12]

量子化法	内容
α	切り捨て
β	切り上げ
γ	2倍後四捨五入
⋮	⋮

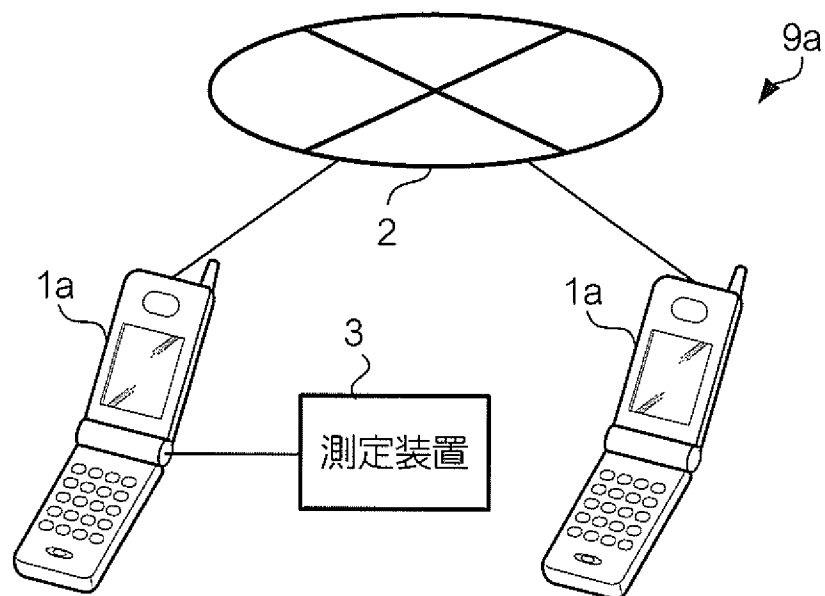
[図13]

配列法	内容
I	左詰
II	右詰
III	パディング
⋮	⋮

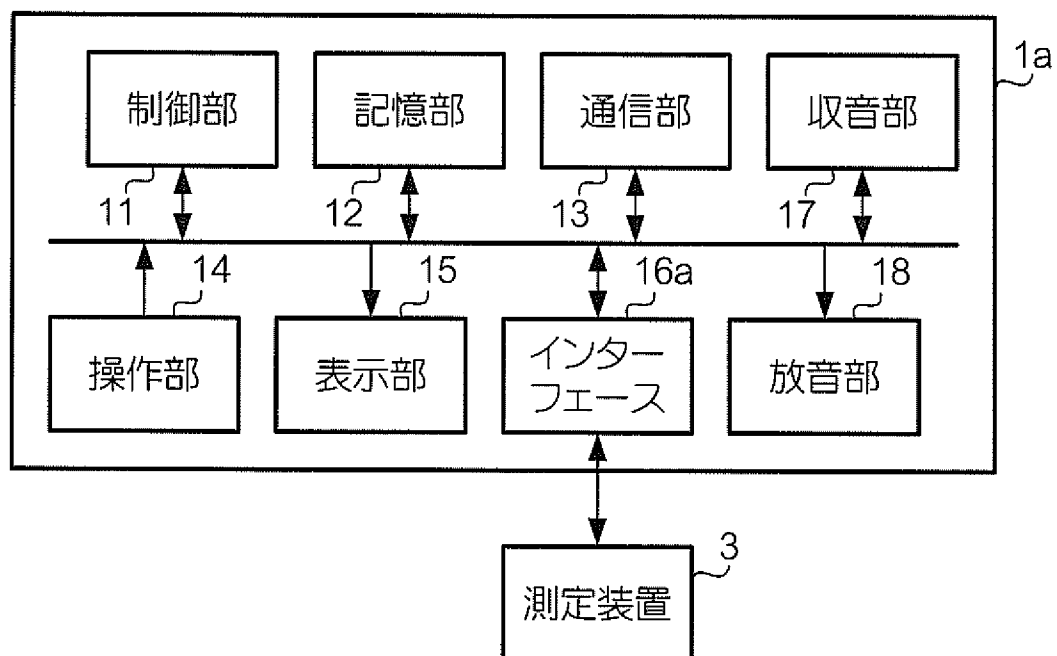
[図14]

測定法	内容
ア	ガスクロマトグラフィー
イ	液体クロマトグラフィー
ウ	赤外分光測定
⋮	⋮

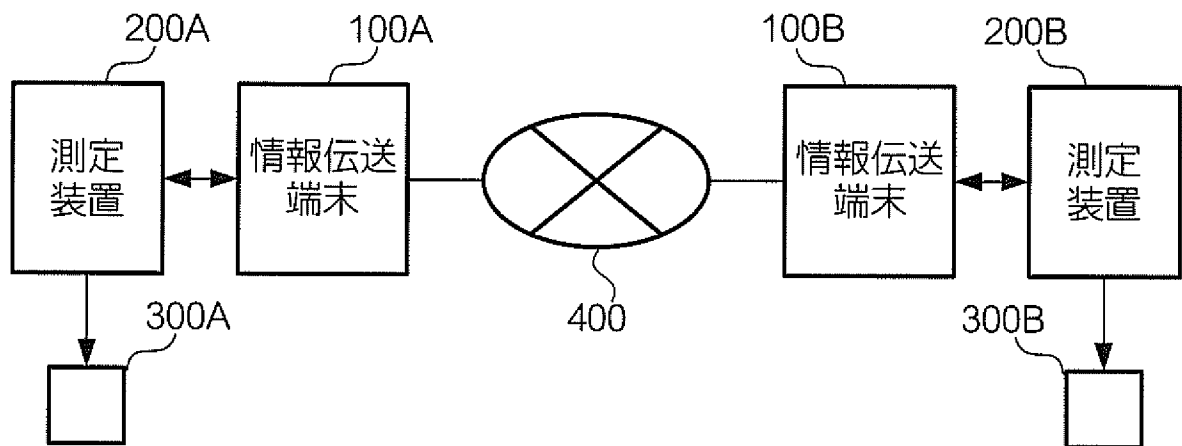
[図15]



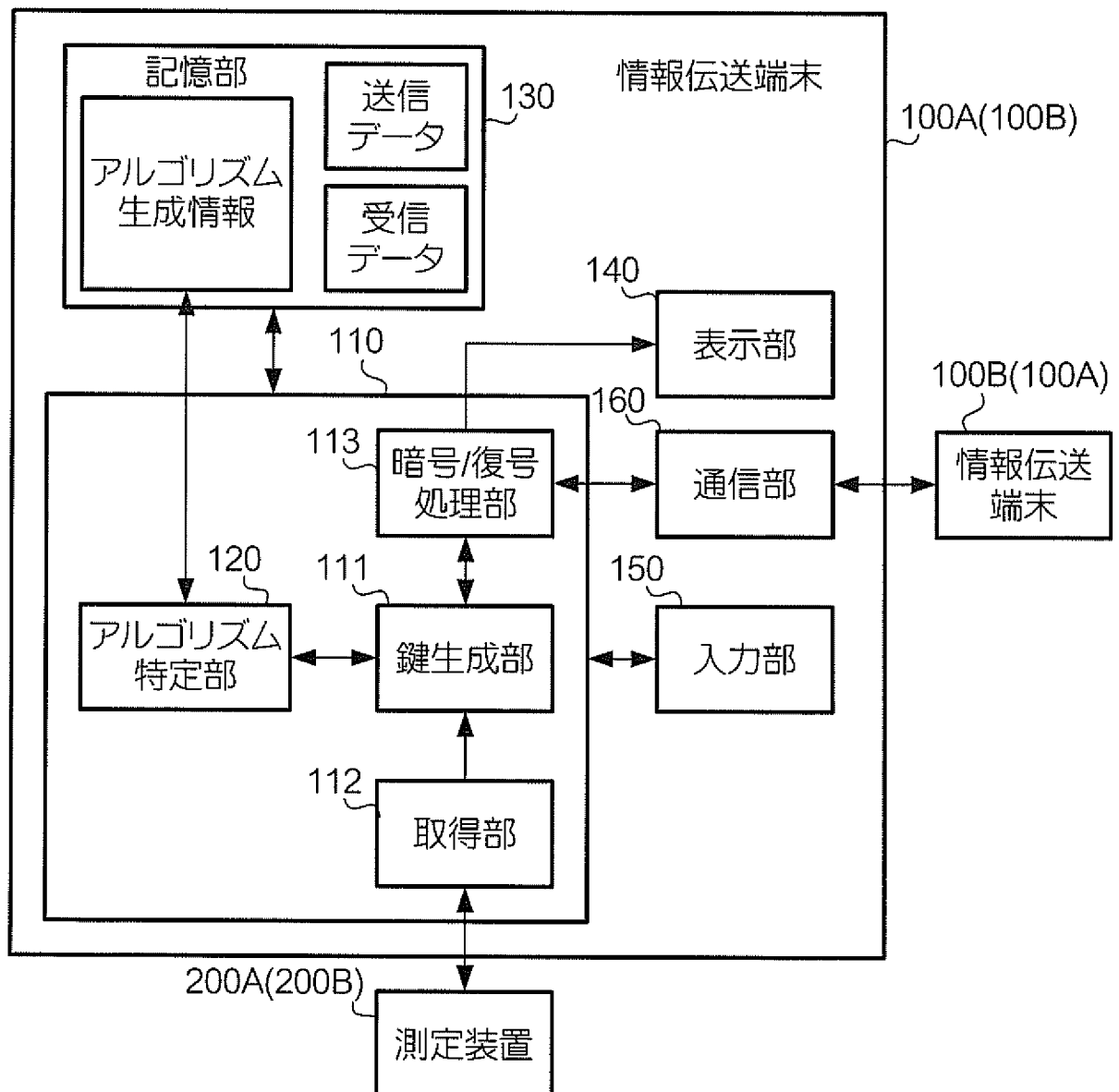
[図16]



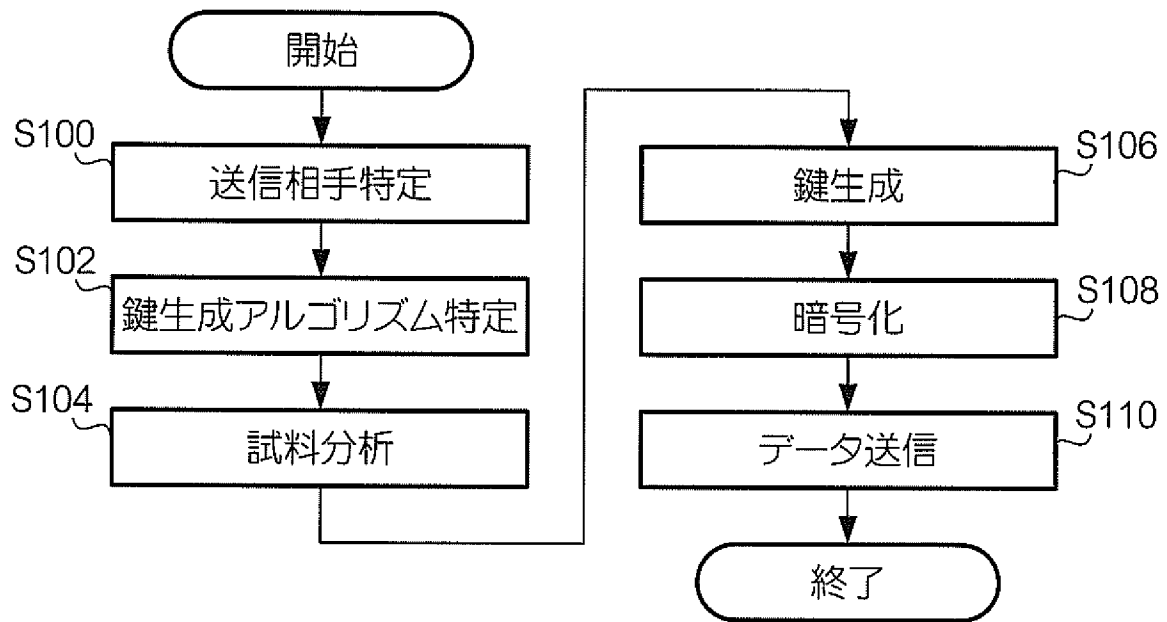
[図17]



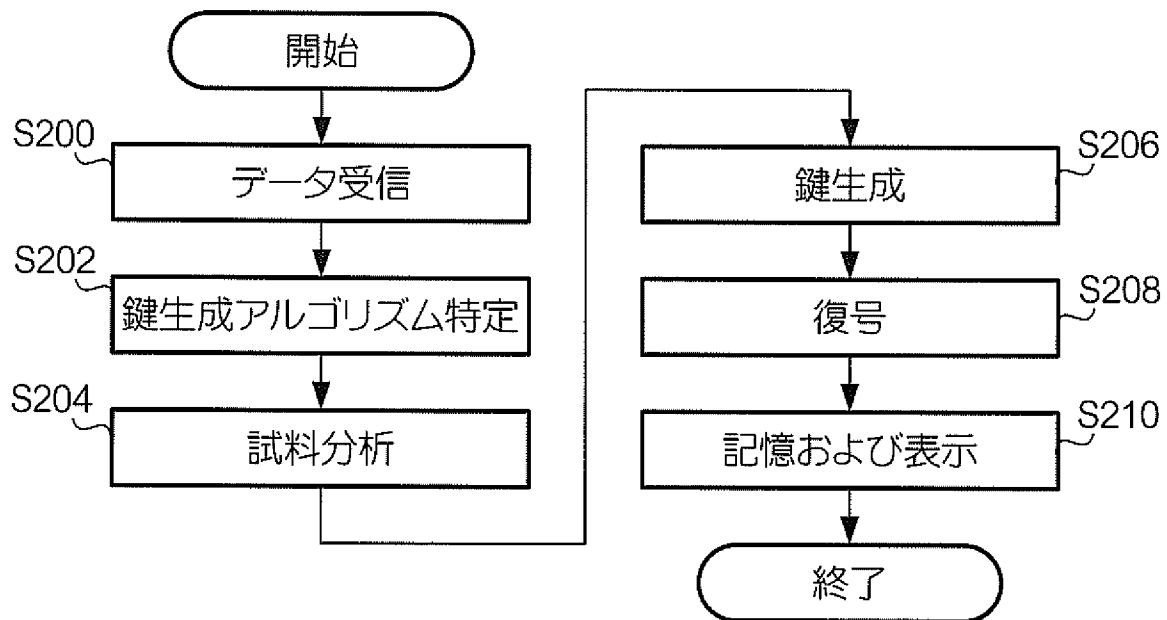
[図18]



[図19]



[図20]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/068614

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2012

Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-53739 A (Zeon Information Systems Co., Ltd.), 23 February 2001 (23.02.2001), paragraphs [0010] to [0013] & EP 1204237 A1 & WO 2001/013570 A1	1-17
Y	WO 2004/003839 A1 (Shin'ya FUKUI et al.), 08 January 2004 (08.01.2004), page 5, line 3 to page 9, line 25; page 13, line 9 to page 14, line 21; page 15, line 14 to page 16, line 20 & US 2006/0091220 A1 & EP 1533749 A1 & AU 2003280488 A & CN 1666226 A	1-17



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
03 August, 2012 (03.08.12)Date of mailing of the international search report
14 August, 2012 (14.08.12)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/068614

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 1-212041 A (Hitachi, Ltd.), 25 August 1989 (25.08.1989), page 4, upper left column, line 17 to page 5, lower left column, line 9 (Family: none)	8, 16
A	JP 2010-514227 A (Signoptic Technologies SAS), 30 April 2010 (30.04.2010), paragraphs [0116] to [0129] & US 2009/0257619 A1 & EP 1971960 B1 & WO 2007/071788 A1 & FR 2895543 A & BRA PI0620363 & CA 2634603 A & CN 101379514 A & AT 529826 T & DK 1971960 T & ES 2374975 T & PT 1971960 E	1-17

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

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

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2012年
日本国実用新案登録公報	1996-2012年
日本国登録実用新案公報	1994-2012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
Y	JP 2001-53739 A（ゼオン情報システム株式会社）2001.02.23, 段落【0010】-【0013】 & EP 1204237 A1 & WO 2001/013570 A1	1-17
Y	WO 2004/003839 A1（福井眞彌，他）2004.01.08, 5頁3行目-9頁25行目、13頁9行目-14頁21行目、 15頁14行目-16頁20行目 & US 2006/0091220 A1 & EP 1533749 A1 & AU 2003280488 A & CN 1666226 A	1-17

☒ 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

03.08.2012

国際調査報告の発送日

14.08.2012

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100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

金沢 史明

5 S

4538

電話番号 03-3581-1101 内線 3546

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
Y	JP 1-212041 A (株式会社日立製作所) 1989.08.25, 4 頁左上欄 17 行目-5 頁左下欄 9 行目 (ファミリーなし)	8, 16
A	JP 2010-514227 A (シグノプティク テクノロジーズ) 2010.04.30, 段落 【0116】 - 【0129】 & US 2009/0257619 A1 & EP 1971960 B1 & WO 2007/071788 A1 & FR 2895543 A & BRA PI0620363 & CA 2634603 A & CN 101379514 A & AT 529826 T & DK 1971960 T & ES 2374975 T & PT 1971960 E	1-17