(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
2009 年1 月29 日 (29.01.2009)

PCT

(10) 国際公開番号
WO 2009/014063 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2008/062929

(22) 国際出願日: 2008 年7 月17 日 (17.07.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2007-189337 2007 年7 月20 日 (20.07.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1080014 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 中山 悟志 (NAKAYAMA, Satoshi) [JP/JP]; 〒1080014 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 山下 穣平 (YAMASHITA, Johei); 〒1050001 東京都港区虎ノ門五丁目１３番１号虎ノ門４０ＭＴビル 山下国際特許事務所 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, 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, 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.

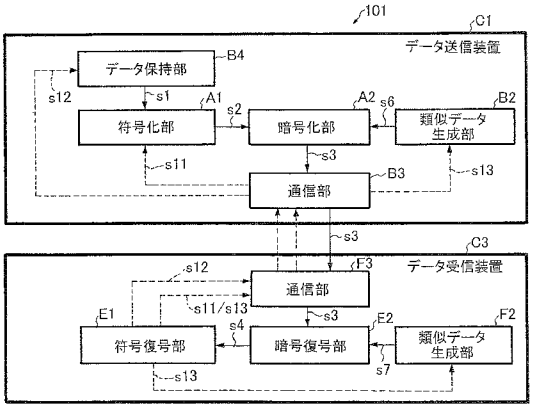
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,

[続葉有]

(54) Title: ENCRYPTED COMMUNICATION METHOD AND ENCRYPTED COMMUNICATION SYSTEM

(54) 発明の名称: 暗号通信方法及び暗号通信システム

[図1]



C1... DATA TRANSMISSION DEVICE
B4... DATA HOLDING UNIT
A1... ENCODING UNIT
A2... ENCRYPTION UNIT
B2... SIMILAR DATA GENERATION UNIT
B3... COMMUNICATION UNIT
C3... DATA RECEPTION DEVICE
E1... DECODING UNIT
F3... COMMUNICATION UNIT
E2... DECRYPTION UNIT
F2... SIMILAR DATA GENERATION UNIT

(57) Abstract: An encrypted communication method includes: a step of generating first and second similar data which are similar to each other; a step of converting communication data to be supplied from a transmission station to a reception station into encoded data by a redundant process based on an encoded parameter for an error correction process; a step of converting the encoded data into encrypted data by an encryption process using the first similar data as a key; a step of transmitting the encrypted data from the transmission station to the reception station; a step of converting the encrypted data received by the reception station into the decrypted data by a decryption process using the second similar data as a key; a step of executing the error correction process of the decrypted data according to the encoded parameter; and a step of recognizing the data obtained when the error correction process is successful, as the communication data.

(57) 要約: 暗号通信方法は、相互に類似する第１および第２の類似データを生成するステップと、誤り訂正処理のための符号化パラメータに基づく冗長化処理により、送信局から受信局へ供給すべき通信データを符号化データに変換するステップと、前記符号化データを前記第１の類似データを鍵として用いた暗号化処理により暗号化データに変換するステップと、前記暗号化データを前記送信局から前記受信局へ送信するステップと、前記受信局が受信した前記暗号化データを前記第２の類似データを鍵として用いた復号処理により復号データに変換するステップと、前記符号化パラメータに基づき前記復号データの誤り訂正処理を実行するステップと、前記誤り訂正処理が成功した場合に得られたデータを前記通信データとして認識するステップとを含む。

WO 2009/014063 A1

CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

暗号通信方法及び暗号通信システム

技術分野

[0001] 本発明は、送信局および受信局間の暗号通信に関する。

背景技術

[0002] 無線LAN(Local Area Network)や無線PAN(Personal Area Network)のように、伝送中のデータが第三者に漏洩しやすいネットワークのセキュリティを強化するために、暗号通信技術が普及している。例えば、無線通信の場合、高速な暗号化／復号の処理が可能な対称鍵方式が好適である。対称鍵方式は、送信局及び受信局が、それらの間で共通に設定された鍵により、通信データを暗号化／復号するというものである。

[0003] 対称鍵方式で用いる共通鍵は、通信しようとするユーザ間で、第三者に漏洩しないように設定し管理される必要がある。共通鍵の取り扱いに関する技術として、例えば、後述の特許文献1に記載のものがある。同文献に記載の技術は、各ユーザの端末をセンターとしてのサーバに接続し、このサーバが各端末に対し、共通鍵を作成するための情報を配布するというものである。各端末は、配布された情報を用いて共通鍵を作成した後、その共通鍵により相互間で暗号通信を行う。

[0004] 特許文献1:特開2006－210968号公報(段落0018-0019、図1)

発明の開示

発明が解決しようとする課題

[0005] 特許文献1に記載の技術によれば、上記のサーバが設けられることにより、共通鍵を作成する際の各端末の計算量が低減される。

[0006] しかしながら、文献1の技術にあっては、上記の機能を持つサーバを、各ユーザの端末とは別個に、ネットワークに接続する必要がある。よって、ネットワークが大型化しやすくコストも掛かることから、SOHOやホームネットワークのような小規模ネットワークには不向きである。また、各ユーザは、共通鍵が設定されるまでに、通信相手の端末のみならずサーバに対しても所定の通信操作を必要とされる。そのため、暗号通

信のためのユーザ操作が煩雑になる可能性がある。

[0007] 本発明の目的は、ネットワークの規模にかかわらず簡便に暗号通信を実行するための技術を提供することにある。

課題を解決するための手段

[0008] 本発明に係る暗号通信方法は、相互に類似する第1および第2の類似データを生成し、誤り訂正処理のための符号化パラメータに基づく冗長化処理により、送信局から受信局へ供給すべき通信データを符号化データに変換し、前記符号化データを前記第1の類似データを鍵として用いた暗号化処理により暗号化データに変換し、前記暗号化データを前記送信局から前記受信局へ送信し、前記受信局が受信した前記暗号化データを前記第2の類似データを鍵として用いた復号処理により復号データに変換し、前記符号化パラメータに基づき前記復号データの誤り訂正処理を実行し、前記誤り訂正処理が成功した場合に得られたデータを前記通信データとして認識するという方法である。

[0009] 本発明に係る暗号通信システムは、送信装置と受信装置とを備え、前記送信装置は、相互に類似する第1および第2の類似データのうちの前記第1の類似データを生成する第1の類似データ生成部と、自装置から前記受信装置へ供給すべき通信データを誤り訂正処理のための符号化パラメータに基づく冗長化処理により符号化データに変換する符号化部と、前記符号化データを前記第1の類似データを鍵として用いた暗号化処理により暗号化データに変換する暗号化部と、前記暗号化データを前記受信装置へ送信する通信部とを有し、前記受信装置は、前記第2の類似データを生成する第2の類似データ生成部と、前記送信装置から受信した暗号化データを前記第2の類似データを鍵として用いた復号処理により復号データに変換する暗号復号部と、前記符号化パラメータに基づき前記復号データの誤り訂正処理を実行し且つ当該誤り訂正処理が成功した場合に得られたデータを前記通信データとして認識する符号復号部とを有する。

[0010] 本発明に係る送信装置は、相互に類似する第1および第2の類似データのうちの前記第1の類似データを生成する類似データ生成部と、自装置から受信装置へ供給すべき通信データを誤り訂正処理のための符号化パラメータに基づく冗長化処理によ

り符号化データに変換する符号化部と、前記符号化データを前記第1の類似データを鍵として用いた暗号化処理により暗号化データに変換する暗号化部と、前記暗号化データを前記受信装置へ送信する通信部とを備える。

[0011] 本発明に係る受信装置は、相互に類似する第1および第2の類似データのうちの前記第2の類似データを生成する類似データ生成部と、前記第1の類似データを鍵として用いた暗号化処理により得られた暗号化データを送信装置から受信したときに当該暗号化データを前記第2の類似データを鍵として用いた復号処理により復号データに変換する暗号復号部と、前記送信装置と共通の符号化パラメータに基づき前記復号データの誤り訂正処理を実行し、且つ、当該誤り訂正処理が成功した場合に得られたデータを前記送信装置から自局へ供給されるべき通信データであると認識する符号復号部とを備える。

発明の効果

[0012] 本発明によれば、ネットワークの規模にかかわらず、送信局及び受信局間の暗号通信を簡便に実行することができる。

図面の簡単な説明

[0013] [図1]本発明の第1の実施形態のシステム構成を示すブロック図である。

[図2]本発明の実施形態における類似データ生成装置のブロック図である。

[図3]本発明の実施形態における類似データ生成装置の外観図である。

[図4]本発明の実施形態における類似データ生成装置の説明図である。

[図5]本発明の第1の実施形態におけるデータ送信装置のフローチャートである。

[図6]本発明の第1の実施形態におけるデータ受信装置のフローチャートである。

[図7]本発明の第1の実施形態における暗号化・復号処理に関する説明図である。

[図8]本発明の第1の実施形態における暗号化・復号処理に関する説明図である。

[図9]本発明の第1の実施形態におけるデータ受信装置のフローチャートである。

[図10]本発明の第1の実施形態におけるデータ受信装置のフローチャートである。

[図11]本発明の第2の実施形態のシステム構成を示すブロック図である。

[図12]本発明の第2の実施形態におけるシステムのシーケンス図である。

符号の説明

[0014] 101、102 システム

C1 データ送信装置

C3 データ受信装置

s1 通信データ

s2 符号化データ

s3 暗号化データ

s4 復号データ

s5 誤り訂正の処理結果

s6 送信局の類似データ

s7 受信局の類似データ

s11 符号化パラメータの更新要求

s12 通信データの再出力要求

s13 類似データの変更要求

s1－1、s5－1 共通鍵

発明を実施するための最良の形態

[0015] ＜第1の実施の形態＞

図1に、本発明の第1の実施形態のシステム構成を示す。本実施形態のシステム101は、送信局及び受信局としてのデータ送信装置C1及びデータ受信装置C3を備える。

[0016] データ送信装置C1は、データ保持部B4、符号化部A1、暗号化部A2、類似データ生成部B2、及び、通信部B3を有する。データ受信装置C3は、通信部F3、類似データ生成部F2、暗号復号部E2、及び、符号復号部E1を有する。

[0017] 類似データ生成部B2および類似データ生成部F2は、相互に類似した値を持つ類似データ(s6,s7)を生成する。類似データs6および類似データs7は、後述の方法により生成される同じビット長のデータであるが、それぞれが示す値は必ずしも同一でなくてよい。また、類似データ生成部B2および類似データ生成部F2は、類似データの変更要求s13を認識した場合、新たに類似データを生成する。

[0018] データ送信装置C1のデータ保持部B4は、データ受信装置C3へ供給すべき通信

データs1を一時的に保持する。データ保持部B4は、通信データの再出力要求s12を認識した場合、前回出力した通信データs1を再び符号化部A1へ供給する。

[0019] 符号化部A1は、自局(C1)からのデータをデータ受信装置C3にて誤り訂正できるようにするために、所定の符号化パラメータに基づいて通信データs1に冗長ビットを付加する。この冗長化処理により、通信データs1が符号化データs2に変換される。

[0020] ここで、符号化パラメータとは、符号化の方式、データ長、冗長性の度合いのうちの少なくとも1つに関する規定であり、例えば、「符号化方式:ハミング符号、データビット長:7、冗長ビット長:4」といったものである。符号化パラメータに基づく冗長化処理は、例えば、ハミング符号やパリティビットの付加など、受信局にてデータの誤りを訂正をできるようにするための任意の方法を採用してよい。

[0021] また、符号化部A1は、符号化パラメータの更新要求s11を認識したとき、その要求に応じて、現行の符号化パラメータを新しいものに更新する。そして、新たな符号化パラメータに基づいて通信データs1を符号化データs2に変換する。

[0022] 暗号化部A2は、類似データ生成部B2からの類似データs6を鍵として符号化データs2を暗号化することにより、符号化データs2を暗号化データs3に変換する。暗号化に用いる演算は、例えばビットごとのXOR(排他的論理和)演算や、語ごとの四則演算など、可逆な演算である。

[0023] 通信部B3及び通信部F3は、データ通信を行う機能を有する。データ送信装置C1の通信部B3は、暗号化データs3をデータ受信装置C3へ送信する。データ受信装置C3の通信部F3は、その暗号化データs3を受信する。

[0024] 暗号復号部E2は、通信部F3で受信された暗号化データs3を、類似データ生成部F2からの類似データs7を鍵として復号処理する。これにより、暗号化データs3を復号データs4に変換する。復号のための演算は、暗号化部A2による前述の暗号化処理と対応させる。例えば、暗号化部A2の演算がビットごとのXORである場合は、暗号復号部E2の演算にもビットごとのXORが適用される。

[0025] 符号復号部E1は、データ送信装置C1の符号化部A1と共通の符号化パラメータに基づき復号データs4の誤り訂正処理を行う。その結果、適正に誤り訂正されたデータを本来の通信データ(s1)として認識する。また、誤り訂正に失敗した場合、すな

わち、許容量を超える誤りが復号データs4に含まれていた場合、符号復号部E1は、以下の(a)及び／又は(b)と、(c)とを行う。

[0026] (a)現行の符号化パラメータよりも冗長性が高い新たな符号化パラメータを決定する。そして、データ送信装置C1の符号化部A1に対し、現行の符号化パラメータを新たなものに更新するよう要求する信号(s11)を発行する。

[0027] (b)類似データ生成部F2と、データ送信装置C1の類似データ生成部B2とに対し、類似データを変更するよう要求する信号(s13)を発行する。

[0028] (c)データ送信装置C1のデータ保持部B4に対し、通信データs1を再出力するよう要求する信号(s12)を発行する。

[0029] 本実施形態において、送信局および受信局の各類似データ生成部(B2,F2)は、他方と共通に与えられる物理作用としての振動により発生した現象をもとに、類似データを生成する類似データ生成装置10である。

[0030] 図2に、類似データ生成装置10の構成例を示す。類似データ生成部B2,F2としての2つの類似データ生成装置10は、振動が与えられている期間の加速度を各自で計測し、その計測値から類似データを形成する。そのための構成として、類似データ生成装置10は、加速度センサ11と、類似データ出力部12と、データ抽出部13とを備える。

[0031] 加速度センサ11は、類似データ生成装置10に与えられた振動の加速度を計測し、その計測値である加速度データをデータ抽出部13に出力する。加速度センサ11は、類似データ生成装置10に固定されていても脱着可能な構造であっても良い。

[0032] データ抽出部13は、加速度データを類似データ出力部12に出力する機能を有する。このデータ抽出部13は、A／D変換部14と、バッファ15と、タイミング制御部16とで構成されている。

[0033] A／D変換部14は、加速度センサ11からのアナログの加速度データをデジタルに変換してバッファ15およびタイミング制御部16へ出力する。A／D変換部14に適用するサンプリング周波数やサンプリング感度などのパラメータは、固定されていても良いし、変更可能なものであってもよい。後者の場合は、例えば、類似データ出力部12からA／D変換部14に対しパラメータ変更の指示を出すようにすればよい。

[0034] タイミング制御部16は、バッファ15に加速度データを蓄積する開始タイミングおよび終了タイミングを制御する。本実施形態では、タイミング制御部16が、A／D変換部14から出力されるデータが示す加速度の値を監視し、その値が閾値を超えたときにバッファ15に対して蓄積開始を指示する。その後、所定時間Tが経過したときにバッファ15に対し蓄積終了を指示する。

[0035] バッファ15は、半導体メモリ等の記憶装置を備えており、タイミング制御部16から蓄積開始の指示を受けたときにA／D変換部14からの加速度データを蓄積し始め、その後の蓄積終了の指示をもって蓄積動作を停止する。

[0036] 類似データ出力部12は、データ抽出部13でバッファリングされた加速度データを用いて類似データを形成し、それを前述の暗号化部A2あるいは暗号復号部E2（図1）へ出力する。

[0037] 図3に、類似データ生成装置10の外観を示す。図示の類似データ生成装置10が送信局及び受信局（C1,C3）のそれぞれに与えられる。類似データ生成装置10において、筐体21の一つの面には、他方の類似データ生成装置10の筐体21を結合するための凹状の結合ガイド22および凸状の結合ガイド23が設けられている。これらの結合ガイド（22,23）は、他方の筐体21の結合ガイドを嵌め合わせることができるように形成されている。

[0038] 図3の例では、加速度センサ11は筐体21の中央付近に設置されている。加速度センサ11の配置は、図示のものに限定されないが、2つの類似データ生成装置10を結合したときに双方の加速度センサ11が近接するように配置することが望ましい。

[0039] 図4に、類似データ生成装置10の取り扱い例を示す。類似データを生成する場合、2つの類似データ生成装置10を結合ガイド22,23（図3）により結合し、それを、例えば図4のように人の手で把持して振る。これにより、双方の類似データ生成装置10に対し共通の振動が与えられることから、相互間で類似した加速度データが得られる。各類似データ生成装置10のバッファ15には、同じ期間に得られた加速度データがバッファリングされる。類似データ出力部12は、バッファリングされた加速度データをもとに、所定ビット長の類似データを形成して出力する。

[0040] このように、類似データ生成部B2,F2として、上記の類似データ生成装置10を用い

ることにより、送信局および受信局で用いる類似データを簡便に生成することができる。

[0041] なお、本実施形態では、類似データ生成部(B2,F2)として、振動の加速度をもとに類似データを生成する装置(10)を用いたが、振動以外の物理作用を利用するものであってもよい。その場合、加速度センサに代えて、必要なセンサを使用すれば良い。例えば、角速度センサ、方位センサ、位置センサ、傾きセンサ、圧力センサ、磁気センサ、光センサ、音センサ、宇宙線センサ、雨量センサ、日照センサ、風向センサ、風速センサ、波力センサ、流量センサ、花粉センサ、温度センサ、湿度センサなどが考えられる。

[0042] 図5に示すフローチャート及び図7の説明図に沿って、データ送信装置C1の動作を説明する。まず、類似データ生成部B2が、データ受信装置C3の類似データ生成部F2との間で類似データ(s6,s7)を生成する(ステップST1)。類似データのビット長は、符号化部A1が出力する符号化データs2のビット長と同一に設定されており、本例では16ビット長を想定する。

[0043] ここでは、図7に示すように、類似データs6として“0011 1011 0100 1010”、類似データs7として“0111 1011 0101 1000”がそれぞれ生成されたとする。これらのビット列は同一ではなく、同図で下線が付されている3ビット分、異なっている。

[0044] データ保持部B4は、データ送信装置C1からデータ受信装置C3へ供給すべき通信データs1を記憶する(図5:ステップST2)。本例では、図7に示すように、通信データs1は4ビット長の“0110”であるとする。

[0045] 符号化部A1は、データ保持部B4から供給された通信データs1を符号化パラメータに従って符号化データs2に変換する(ステップST3)。具体的には、例えば、符号化パラメータが「符号化方式:単純多重化、データビット長:4、冗長ビット長:3」である場合、図7に示すような変換表t1に基づいて、通信データs1が冗長化される。この変換表t1によれば、通信データs1のビット“0”は4ビットのビット列“0000”に変換され、ビット“1”は4ビットのビット列“1111”に変換される。したがって、通信データs1“0110”は符号化データs2“0000 1111 1111 0000”に変換される。

[0046] 次に、暗号化部A2が、類似データ生成部B2から供給された類似データs6を鍵と

して、符号化データs2を暗号化する(ステップST4)。これにより、符号化データs2が暗号化データs3に変換される。具体的には、図7より、符号化データs2“0000 1111 1111 0000”と、類似データs6“0011 1011 0100 1010”との1ビットずつのXORにより、暗号化データs3“0011 0100 1011 1010”が得られる。

[0047] 通信部B3は、暗号化データs3をデータ受信装置C3へ送信する(ステップST5)。以降のデータ送信装置C1の処理(ステップST31～)については、後に説明する。

[0048] 図6に示すフローチャートに沿って、データ受信装置C3の動作を説明する。まず、類似データ生成部F2が、前述した手順により、データ送信装置C1の類似データ生成部B2との間で類似データ(s6,s7)を生成する(ステップST11)。

[0049] データ送信装置C1からの暗号化データs3を通信部F3が受信すると(ステップST12)、暗号復号部E2が、その暗号化データs3を類似データs7により復号する(ステップST13)。これにより、復号データs4が得られる。具体的には、図7より、暗号化データs3“0011 0100 1011 1010”と、類似データs7“0111 1011 0101 1000”との1ビットずつのXORにより、復号データs4“0100 1111 1110 0010”が得られる。

[0050] 符号復号部E1は、符号化パラメータに従って復号データs4の誤り訂正処理を行う(ステップST14)。この符号化パラメータは、前述の符号化部A1が使用する符号化パラメータと共通のものである。符号復号部E1は、図7の変換表t2に基づいて復号データs4の誤り訂正を行う。

[0051] 変換表t2によれば、“0001”のように“1”が1つ含まれるコードと、コード“0000”とが、メッセージ“0”に変換される。また“1110”のように“0”が1つ含まれるコードと、コード“1111”とが、メッセージ“1”に変換される。したがって、復号データs4“0100 1111 1110 0010”が誤り訂正処理されると、その処理結果s5として“0110”が得られる。

[0052] 符号復号部E1は、復号データs4の誤り訂正が成功した場合(ステップST15:Yes)、すなわち、上記のように復号データs4を4ビット長のデータ(s5)に変換できた場合、そのデータを、送信局が意図する通信データs1として認識する(ステップST16)。

[0053] 一方、復号データs4を変換表t2により変換することができない場合、符号復号部E1は、復号データs4の誤りビット数が許容量を超えるため、誤り訂正に失敗したと認識する(ステップST15:No)。

[0054] 図8に、誤り訂正が失敗するケースを挙げる。図示の通信データs1および変換表t1,t2は、いずれも前述した図7のものと同様である。このケースでは、前述のケースとは異なり、送信局の類似データs6として“1001 1010 0001 1001”が生成され、受信局の類似データs7として“1001 1110 0010 1001”が生成されている。これらのビット列は、図8で下線が付されている3ビット分、異なっている。

[0055] 通信データs1“0110”が符号化データs2“0000 1111 1111 0000”に変換されると、暗号化データs3を得るために、符号化データs2と上記の類似データs6とによる1ビットずつのXORが算出される。その結果、暗号化データs3として“1001 0101 1110 1001”が得られる。

[0056] 上記の暗号化データs3が受信局(C3)に届くと、この受信局で保持する類似データs7“1001 1110 0010 1001”と暗号化データs3との1ビットずつのXORにより、復号データs4“0000 1011 1100 0000”が得られる。

[0057] 符号復号部E1は、上記復号データs4の誤り訂正処理を行うべく、変換表t2により復号データs4の変換を試みる。しかしながら、図8に示すように、復号データs4の9ビット目から12ビット目で構成されるビット列“1100”については、対応するコードが変換表t2に存在しない。よって、復号データs4を適正なメッセージに変換することができない。このような場合、符号復号部E1は、復号データs4の誤りを訂正することができないと認識する。

[0058] 図9及び図10に示すフローチャートに沿って、復号データs4の誤り訂正が失敗した場合のデータ送信装置C1及びデータ受信装置C3の動作を説明する。

[0059] データ受信装置C3の符号復号部E1は、復号データs4の誤り訂正に失敗したことを認識すると、適正な通信データs1を得るために、前述した(a)又は(b)の処理を実行する。いずれの処理を採るかは、事前に設定しておく。なお、本実施形態では(a)及び(b)の何れか一方を採るが、これら両方の処理を実行するようにしてもよい。

[0060] 上記処理のうちの(b)、すなわち現行の符号化パラメータを維持しつつ類似データを変更するという処理が採られる場合(ステップST21:Yes)、符号復号部E1は、データ送信装置C1および自局の類似データ生成部F2に対し、類似データの変更要求s13を発行する(ステップST22)。

[0061] 類似データ生成部F2は、データ送信装置C1の類似データ生成部B2との間で新たな類似データを生成する(ステップST23)。符号復号部E1は、データ送信装置C1に対し、前回と同じ通信データs1の再出力要求s12を発行する(ステップST24)。

[0062] また、(a)の処理、すなわち現行の符号化パラメータを変更する場合(ステップST21:No)、符号復号部E1は、自局(C3)の符号化パラメータの設定を、より冗長度の高いものに変更する(ステップST25)。具体的には、例えば前述の「符号化方式:単純多重化、データビット長:4、冗長ビット長:3」という設定を、「符号化方式:単純多重化、データビット長:5、冗長ビット長:4」に変更する等である。

[0063] 符号復号部E1は、自局での変更と同様な変更をデータ送信装置C1に指示すべく、データ送信装置C1に対し符号化パラメータの更新要求s11を発行する(ステップST26)。また、通信データs1の再出力要求s12も発行する(ステップST24)。その後、再出力された通信データs1に基づく暗号化データs3がデータ送信装置C1から送信されると、データ受信装置C3は、新たな類似データあるいは新たな符号化パラメータを用いて、前述のステップS12(図6)以降の処理を実行する。

[0064] 一方、データ送信装置C1は、上記(b)が採用されることにより、データ受信装置C3から類似データの変更要求s13を受信した場合(図10のステップST31:Yes)、類似データ生成部B2が、データ受信装置C3の類似データ生成部F2との間で新たな類似データを生成する(ステップST32)。

[0065] また、上記(a)の採用により、データ送信装置C1がデータ受信装置C3から符号化パラメータの更新要求s11を受信した場合は(ステップST33:Yes)、符号化部A1が、その要求に応じて自局の符号化パラメータを新しいものに更新する(ステップST34)。

[0066] 新たな類似データを作成(ステップST32)、あるいは、符号化パラメータを更新(ステップST34)した後、データ受信装置C3から通信データの再出力要求s12を受信すると(ステップST35)、データ送信装置C1は、データ保持部B4により前回と同じ通信データs1を符号化部A1へ供給する。そして、新たな類似データあるいは新たな符号化パラメータを用いて、前述のステップST3(図5)以降の処理を実行する。

[0067] 本実施形態によれば、ネットワークの規模にかかわらず送信局及び受信局間の暗

号通信を簡便に実行することができる。また、送信局から受信局への通信データの誤り訂正が失敗しても、新たな符号化パラメータや類似データにより、その通信データの誤り適正処理が再試行されるので、受信局に対し適正な通信データを受け渡すことができる。

[0068] ＜第2の実施の形態＞

[0069] 図11に、本発明の第2の実施形態のシステム構成を示す。本実施形態のシステム102は、第1の実施形態のシステム101（図1）と比較して、次の点が異なる。

[0070] システム102は、さらに、データ送信装置C1に対し共通鍵を発行する鍵生成装置C5と、共通鍵を用いて暗号通信を行う暗号通信装置C2,C4とを備える。これらの装置は、それぞれに対応するデータ送信装置C1及びデータ受信装置C3に対し、別個の装置として構成することに代えて、一体化してもよい。

[0071] 本実施形態のデータ送信装置C1は、鍵生成装置C5から発行された共通鍵s1－1を保存する鍵保持部B4－1を備える。この鍵保持部B4－1のハードウェア構成は、前述のデータ保持部B4（図1）と同様のものを用いることができる。

[0072] 図12に示すシーケンスに沿って、システム102の動作を説明する。まず、鍵生成装置C5が、データ送信装置C1及び暗号通信装置C2に対し共通鍵s1－1を発行する（ステップST41）。暗号通信装置C2は、共通鍵s1－1を暗号通信の鍵として設定する（ステップST42）。データ送信装置C1は、共通鍵s1－1を鍵保持部B4－1に保存する（ステップST43）。

[0073] このあと、共通鍵s1－1をデータ送信装置C1からデータ受信装置C3へ受け渡す処理が行われる（ステップST44）。この処理は、前述の第1の実施形態のものに準じる。すなわち、第1の実施形態での通信データ（s1）を共通鍵s1－1に置き換え、類似データ（s6,s7）を用いた暗号通信により、共通鍵s1－1をデータ送信装置C1からデータ受信装置C3へ受け渡す。

[0074] 復号データ（s4）の誤り訂正処理が成功すると、データ受信装置C3は、処理結果のデータs5－1が共通鍵であると認識し（ステップST45）、それを暗号通信装置C4へ供給する（ステップST46）。暗号通信装置C4は、供給されたデータs5－1を、暗号通信装置C2との暗号通信に用いる共通鍵として設定する（ステップST47）。

[0075] 上記の処理により共通鍵(s1－1,s5－1)が暗号通信装置C2,C4のそれぞれに設定されると、暗号通信装置C2,C4は、その共通鍵を用いた暗号化処理および復号処理によりデータ通信を実行する(ステップST48)。

[0076] 本実施形態によれば、暗号通信に用いる共通鍵を送信局から受信局へ簡便かつ安全に受け渡すことができる。

[0077] 本発明の実施は、上記形態に限定されるものではなく、本願の請求の範囲内において、適宜変更が可能である。例えば、本発明は、データ送信装置(C1)あるいはデータ受信装置(C3)の動作に対応したコンピュータプログラム、又は、そのプログラムを記憶した記録媒体として実施することができる。

[0078] また、本発明の実施にあたり、類似データを生成する手段は、類似データ生成装置10(図4)のように物理現象をもとに類似データを生成する装置に限定されない。例えば、類似データ生成部B2,F2をそれぞれ量子暗号通信装置で実現することもできる。この場合、データ送信装置C1の類似データ生成部B2が乱数などにより生成したデータAを類似データs6とし、このデータAを量子暗号通信によってデータ受信装置C3へ送信する。そして、データ受信装置C3の類似データ生成部F2が、データAを復号してデータBを取得し、これを類似データs7として暗号復号部E2に渡す。

[0079] 本発明に係るシステム構成は、前述の各実施形態のように送信局／受信局を一対一に接続する構成に限らず、一対多、すなわち、例えば1つの送信局に対し複数の受信局を接続するという構成であってもよい。その場合、類似データ生成装置10において、筐体21(図3)の複数の面に結合ガイド22,23を設けることで、3つ以上の筐体を結合することができる。これにより、3つ以上の類似データ生成装置10に対し、共通の振動を与えることができる。

[0080] 本発明において、送信局／受信局間の通信形態は、無線または有線、あるいは、それらの組み合わせの何れであってもよい。

[0081] 本出願は、2007年7月20日に日本出願された特願2007－189337を基礎とする優先権を主張し、その開示の内容を全て本明細書に取り込むものである。

請求の範囲

[1] 相互に類似する第1および第2の類似データを生成し、

誤り訂正処理のための符号化パラメータに基づく冗長化処理により、送信局から受信局へ供給すべき通信データを符号化データに変換し、

前記符号化データを前記第1の類似データを鍵として用いた暗号化処理により暗号化データに変換し、

前記暗号化データを前記送信局から前記受信局へ送信し、

前記受信局が受信した前記暗号化データを前記第2の類似データを鍵として用いた復号処理により復号データに変換し、

前記符号化パラメータに基づき前記復号データの誤り訂正処理を実行し、

前記誤り訂正処理が成功した場合に得られたデータを前記通信データとして認識することを特徴とする暗号通信方法。

[2] 前記誤り訂正処理が失敗した場合、さらに、相互に類似する新たな第1および第2の類似データを生成し、前記新たな各類似データを用いた暗号化処理および復号処理を経た復号データにより前記誤り訂正処理を再試行することを特徴とする請求項1記載の暗号通信方法。

[3] 前記誤り訂正処理が失敗した場合、さらに、前記符号化パラメータをより高い冗長度を持つ新たな符号化パラメータに更新し、前記新たな符号化パラメータにより前記誤り訂正処理を再試行することを特徴とする請求項1又は2記載の暗号通信方法。

[4] さらに、前記送信局に対し前記通信データとしての共通鍵を発行し、

前記共通鍵に関する誤り訂正処理が成功した後、当該共通鍵を用いた暗号化処理および復号処理により前記送信局および受信局間のデータ通信を実行することを特徴とする請求項1乃至3のいずれか1項に記載の暗号通信方法。

[5] 前記第1および第2の類似データを生成するとき、複数の筐体に対する共通の物理作用により当該各筐体に発生する現象を計測し、相互に異なる筐体に関する計測値から所定ビット長のデータを形成し当該データを前記第1または第2の類似データに適用することを特徴とする請求項1乃至4のいずれか1項に記載の暗号通信方法。

[6] 前記共通の物理作用が振動であることを特徴とする請求項5記載の暗号通信方法

。

[7] 送信装置と受信装置とを備え、

前記送信装置は、相互に類似する第1および第2の類似データのうちの前記第1の類似データを生成する第1の類似データ生成部と、自装置から前記受信装置へ供給すべき通信データを誤り訂正処理のための符号化パラメータに基づく冗長化処理により符号化データに変換する符号化部と、前記符号化データを前記第1の類似データを鍵として用いた暗号化処理により暗号化データに変換する暗号化部と、前記暗号化データを前記受信装置へ送信する通信部とを有し、

前記受信装置は、前記第2の類似データを生成する第2の類似データ生成部と、前記送信装置から受信した暗号化データを前記第2の類似データを鍵として用いた復号処理により復号データに変換する暗号復号部と、前記符号化パラメータに基づき前記復号データの誤り訂正処理を実行し且つ当該誤り訂正処理が成功した場合に得られたデータを前記通信データとして認識する符号復号部とを有することを特徴とする暗号通信システム。

[8] 前記符号復号部は、前記誤り訂正処理が失敗した場合、前記第1及び第2の各類似データ生成部に対し、相互に類似する新たな第1および第2の類似データを生成するよう要求し、当該要求により生成された新たな各類似データを用いた暗号化処理および復号処理を経た復号データにより前記誤り訂正処理を再試行することを特徴とする請求項7記載の暗号通信システム。

[9] 前記符号復号部は、前記誤り訂正処理が失敗した場合、前記符号化パラメータをより高い冗長度を持つ新たな符号化パラメータに更新し、当該更新と同様の更新を前記符号化部へ指示し、前記新たな符号化パラメータにより前記誤り訂正処理を再試行することを特徴とする請求項7又は8記載の暗号通信システム。

[10] さらに、前記送信装置に対し前記通信データとしての共通鍵を発行する鍵生成装置と、前記送信装置および前記受信装置に接続された第1および第2の暗号通信装置とを備え、

前記鍵生成装置は、前記送信装置へ発行した共通鍵を前記第1の暗号通信装置へ供給し、

前記符号復号部は、前記共通鍵に関する誤り訂正処理が成功したとき、当該共通鍵を前記第2の暗号通信装置へ供給し、

前記第1および第2の暗号通信装置は、それぞれに供給された共通鍵を用いた暗号化処理および復号処理によりデータ通信を実行することを特徴とする請求項7乃至9のいずれか1項に記載の暗号通信システム。

[11] 前記第1および第2の各類似データ生成部は、物理作用が与えられる筐体と、前記筐体と他方の類似データ生成部の筐体とに対し与えられた共通の物理作用により発生する現象を計測するセンサと、前記センサの計測値を取得する取得部と、前記取得した計測値から所定ビット長のデータを形成し当該データを前記第1または第2の類似データとして出力する出力部とを有することを特徴とする請求項7乃至10のいずれか1項に記載の暗号通信システム。

[12] 前記共通の物理作用が振動であることを特徴とする請求項11記載の暗号通信システム。

[13] 相互に類似する第1および第2の類似データのうちの前記第1の類似データを生成する類似データ生成部と、

自装置から受信装置へ供給すべき通信データを誤り訂正処理のための符号化パラメータに基づく冗長化処理により符号化データに変換する符号化部と、

前記符号化データを前記第1の類似データを鍵として用いた暗号化処理により暗号化データに変換する暗号化部と、

前記暗号化データを前記受信装置へ送信する通信部とを備えることを特徴とする送信装置。

[14] 前記類似データ生成部は、物理作用が与えられる筐体と、前記筐体と前記第2の類似データを生成する他の類似データ生成部の筐体とに対し与えられた共通の物理作用により発生する現象を計測するセンサと、前記センサの計測値を取得する取得部と、前記取得した計測値から所定ビット長のデータを形成し当該データを前記第1の類似データとして出力する出力部とを有することを特徴とする請求項13記載の送信装置。

[15] 前記共通の物理作用が振動であることを特徴とする請求項16記載の送信装置。

[16] 相互に類似する第1および第2の類似データのうちの前記第2の類似データを生成する類似データ生成部と、

前記第1の類似データを鍵として用いた暗号化処理により得られた暗号化データを送信装置から受信したときに当該暗号化データを前記第2の類似データを鍵として用いた復号処理により復号データに変換する暗号復号部と、

前記送信装置と共通の符号化パラメータに基づき前記復号データの誤り訂正処理を実行し、且つ、当該誤り訂正処理が成功した場合に得られたデータを前記送信装置から自局へ供給されるべき通信データであると認識する符号復号部とを備えることを特徴とする受信装置。

[17] 前記符号復号部は、前記誤り訂正処理が失敗した場合、相互に類似する新たな第1および第2の類似データを用いた暗号化処理および復号処理を経た復号データにより前記誤り訂正処理を再試行することを特徴とする請求項16記載の受信装置。

[18] 前記符号復号部は、前記誤り訂正処理が失敗した場合、前記符号化パラメータをより高い冗長度を持つ新たな符号化パラメータに更新し、当該更新と同様の更新を前記送信装置へ指示し、前記新たな符号化パラメータにより前記誤り訂正処理を再試行することを特徴とする請求項16又は17記載の受信装置。

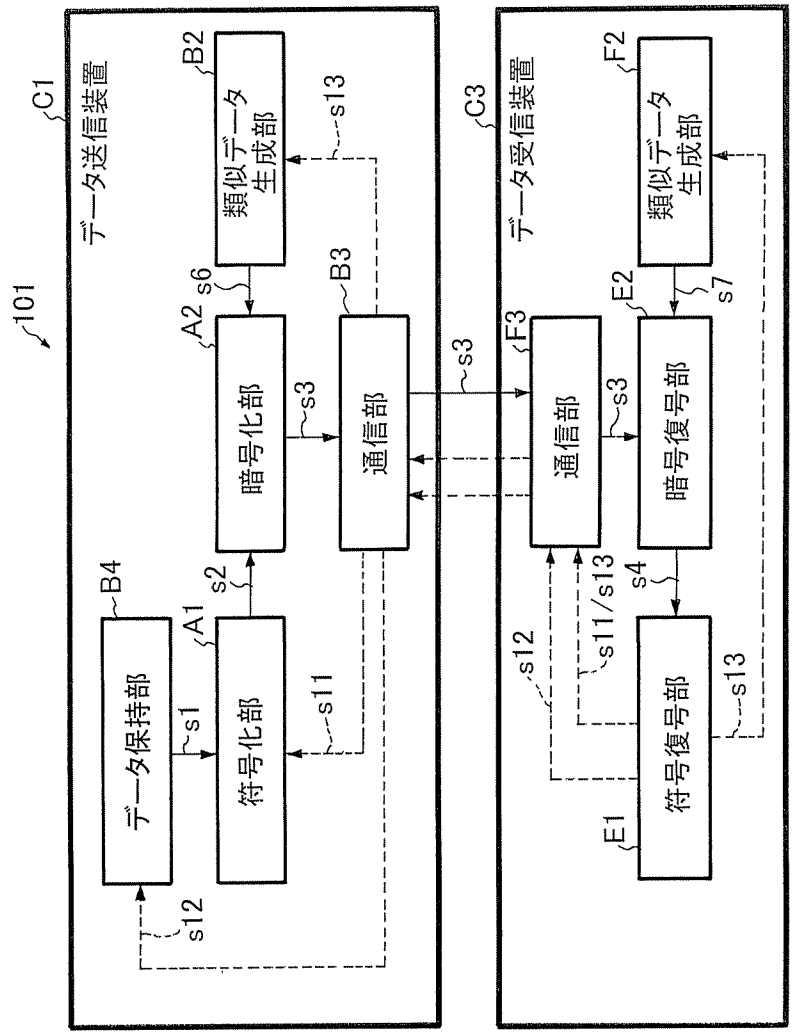
[19] 前記類似データ生成部は、物理作用が与えられる筐体と、前記筐体と前記第1の類似データを生成する他の類似データ生成部の筐体とに対し与えられた共通の物理作用により発生する現象を計測するセンサと、前記センサの計測値を取得する取得部と、前記取得した計測値から所定ビット長のデータを形成し当該データを前記第2の類似データとして出力する出力部とを有することを特徴とする請求項16乃至18のいずれか1項に記載の受信装置。

[20] 前記共通の物理作用が振動であることを特徴とする請求項19記載の受信装置。

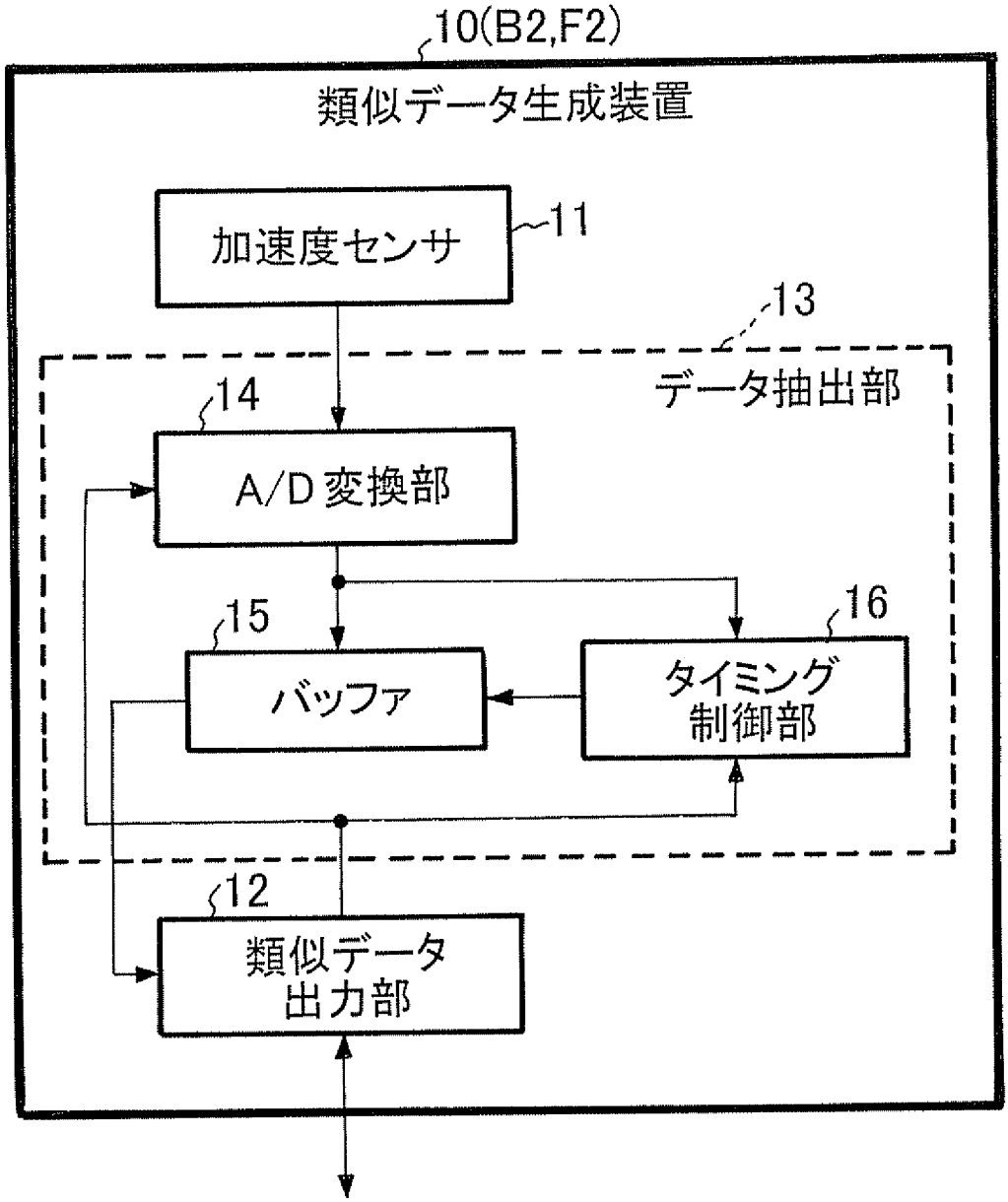
[21] コンピュータを請求項13記載の送信装置として機能させることを特徴とするプログラム。

[22] コンピュータを請求項16乃至18のいずれか1項に記載の受信装置として機能させることを特徴とするプログラム。

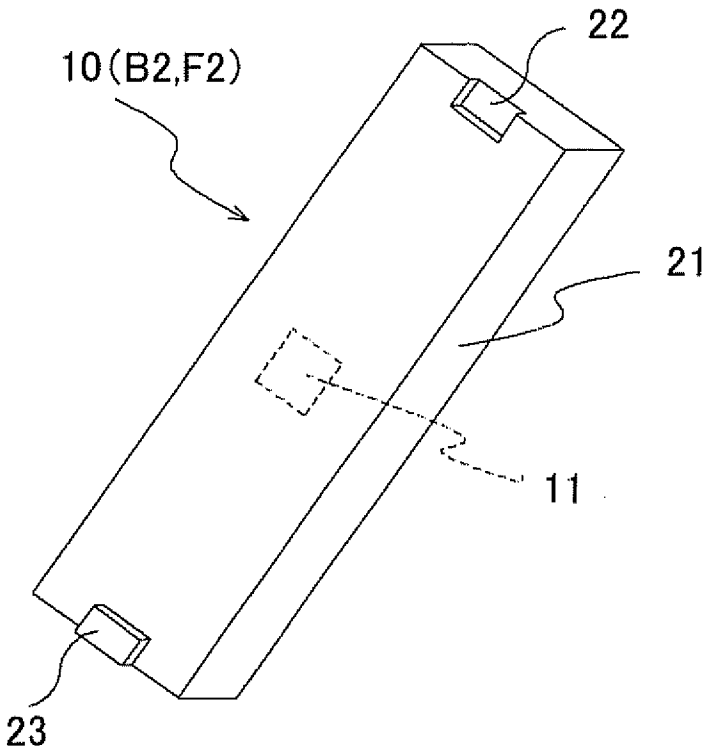
[図1]


101
C1
データ送信装置
B2
類似データ生成部
s13
s6
B3
A2
暗号化部
s3
通信部
s3
B4
s2
A1
データ保持部
s1
符号化部
s11
s12
C3
データ受信装置
F2
類似データ生成部
E2
s7
F3
通信部
s3
暗号復号部
s4
s12
s11/s13
E1
符号復号部
s13

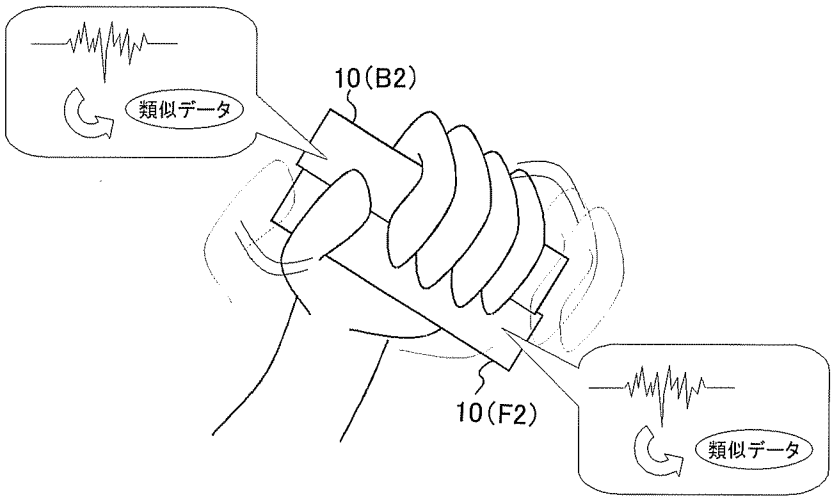
[図2]


10(B2,F2)
類似データ生成装置
加速度センサ
11
13
データ抽出部
14
A/D 変換部
15
バッファ
16
タイミング
制御部
12
類似データ
出力部

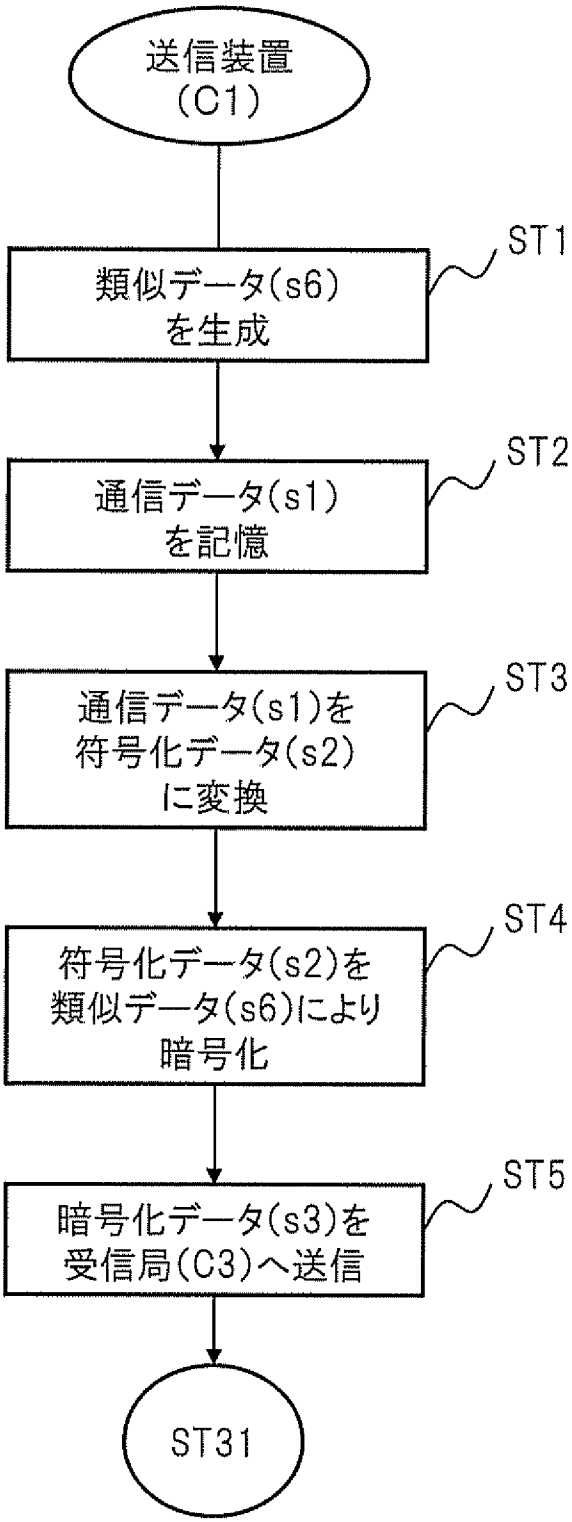
[図3]



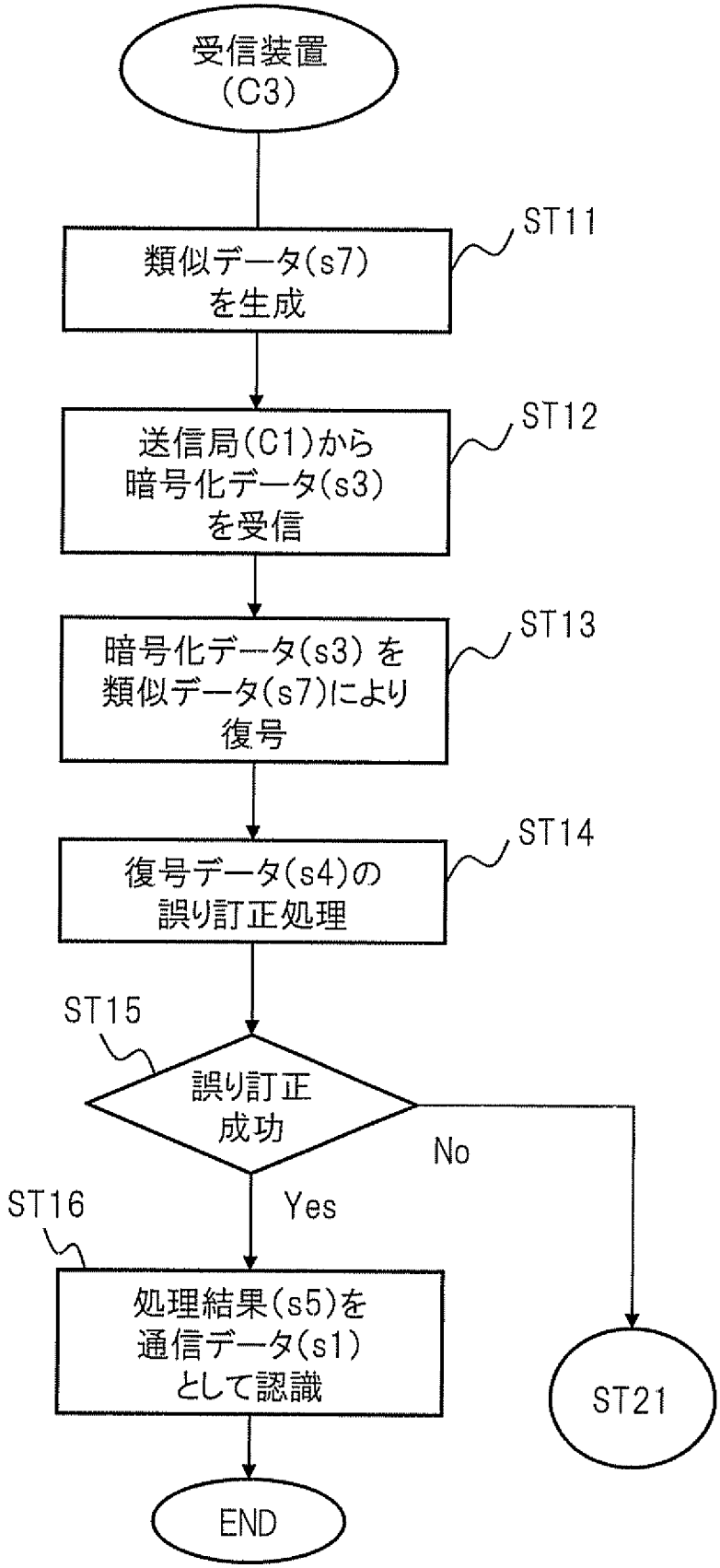
[図4]



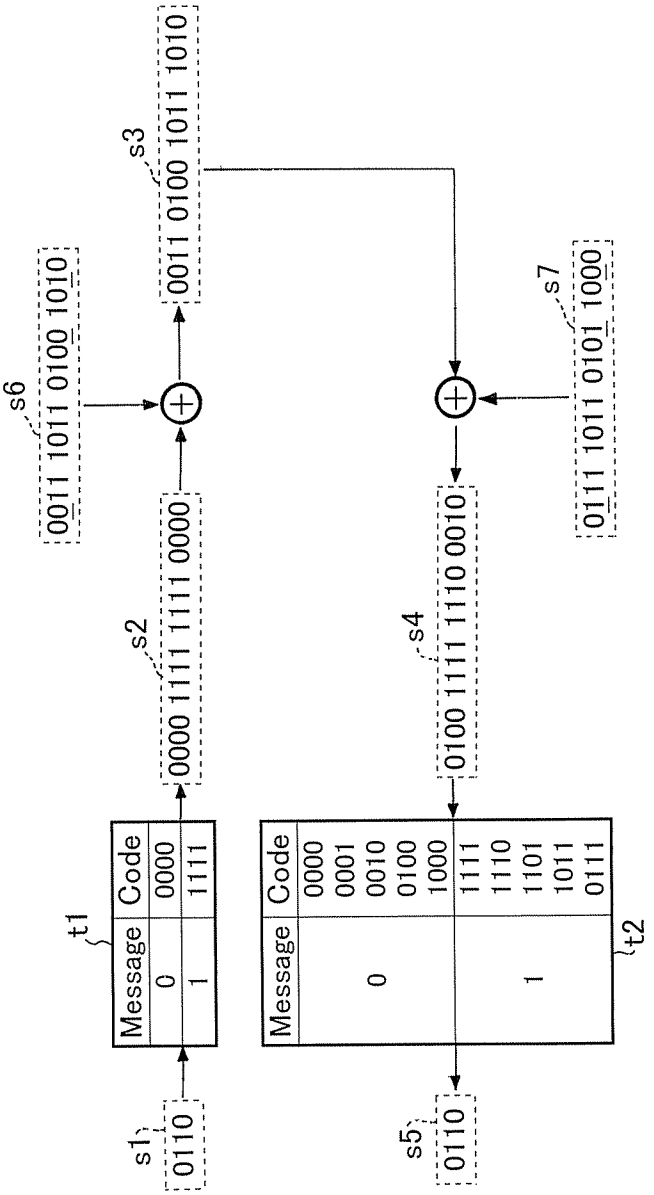
[図5]


送信装置
(C1)
類似データ(s6)
を生成
ST1
通信データ(s1)
を記憶
ST2
通信データ(s1)を
符号化データ(s2)
に変換
ST3
符号化データ(s2)を
類似データ(s6)により
暗号化
ST4
暗号化データ(s3)を
受信局(C3)へ送信
ST5
ST31

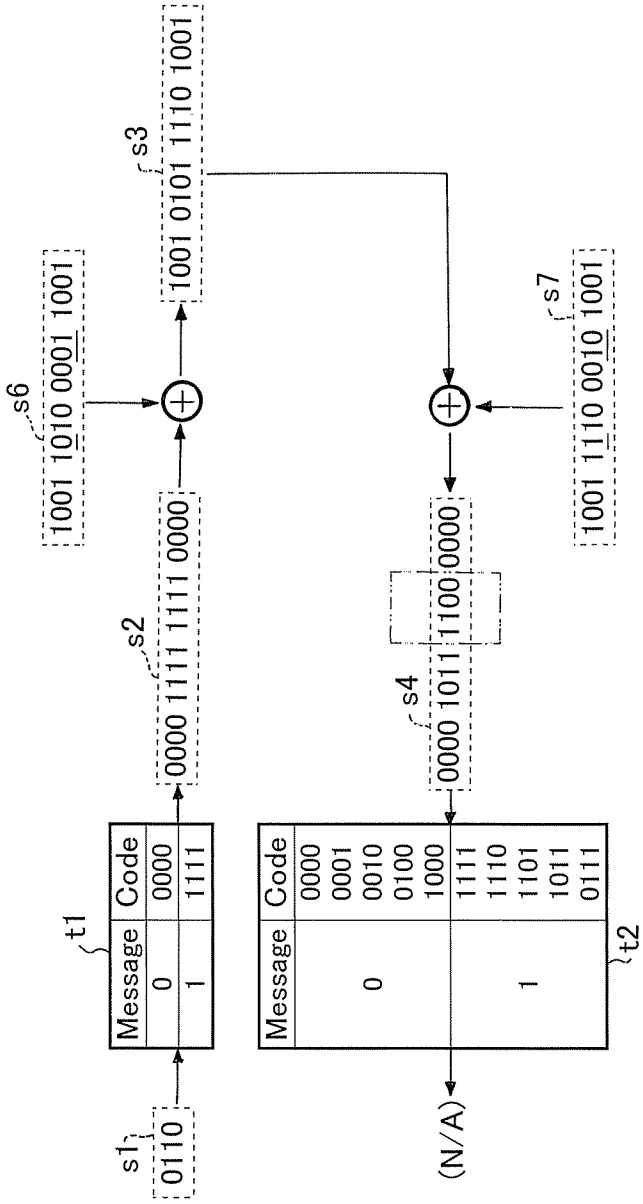
[図6]


受信装置
(C3)
ST11
類似データ(s7)
を生成
ST12
送信局(C1)から
暗号化データ(s3)
を受信
ST13
暗号化データ(s3) を
類似データ(s7)により
復号
ST14
復号データ(s4)の
誤り訂正処理
ST15
誤り訂正
成功
No
Yes
ST16
処理結果(s5)を
通信データ(s1)
として認識
ST21
END

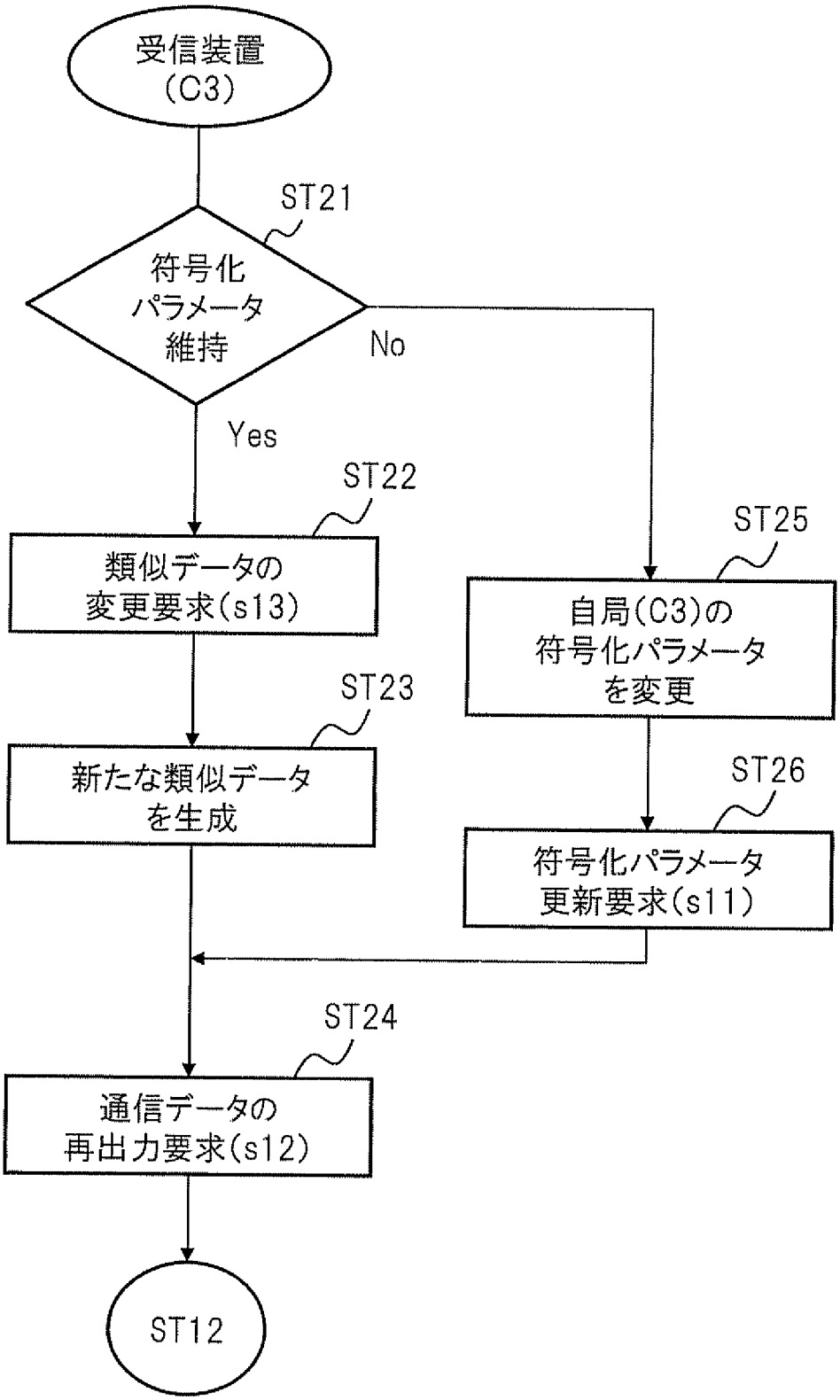
[図7]


s1
0110
t1
Message
Code
0
0000
1
1111
s2
0000 1111 1111 0000
s3
0011 0100 1011 1010
s4
0100 1111 1110 0010
s5
0110
t2
Message
Code
0
0000
0001
0010
0100
1000
1
1111
1110
1101
1011
0111
s6
0011 1011 0100 1010
s7
0111 1011 0101 1000

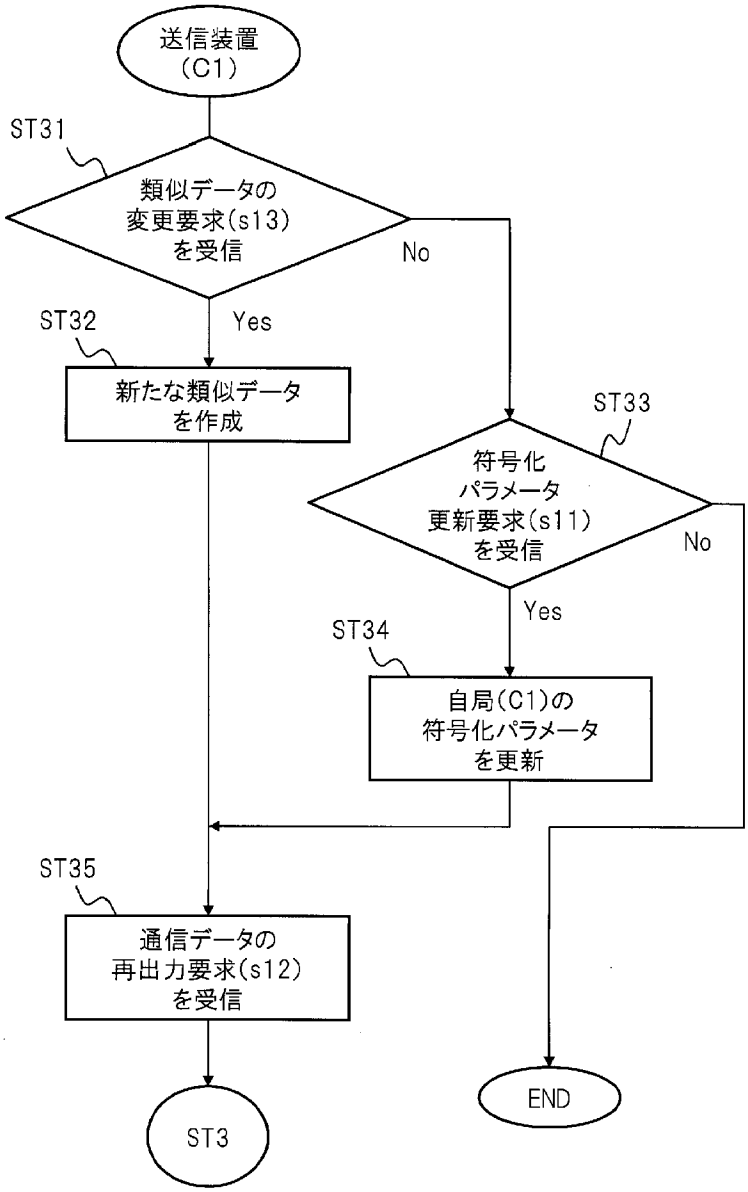
[図8]


s1
0110
t1
Message
Code
0
0000
1
1111
s2
0000 1111 1111 0000
s6
1001 1010 0001 1001
s3
1001 0101 1110 1001
s4
0000 1011 1100 0000
s7
1001 1110 0010 1001
t2
Message
Code
0
0000
0001
0010
0100
1000
1
1111
1110
1101
1011
0111
(N/A)

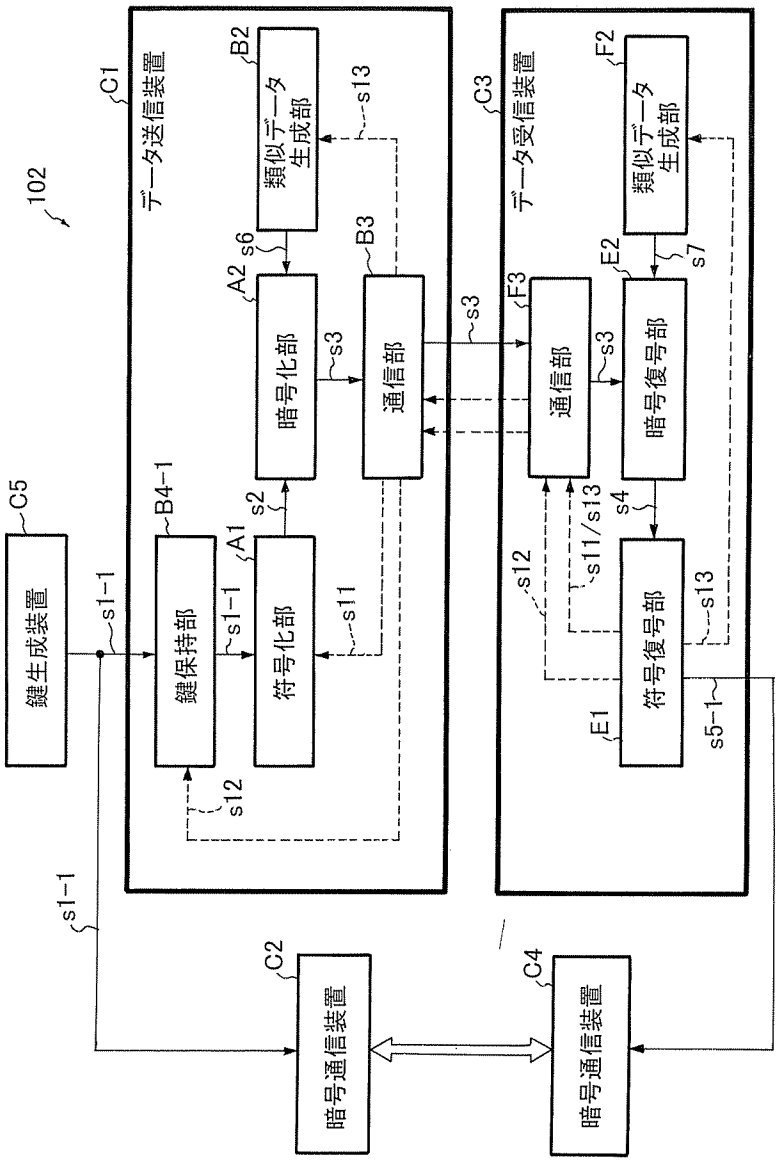
[図9]


受信装置
(C3)
ST21
符号化
パラメータ
維持
No
Yes
ST22
類似データの
変更要求(s13)
ST23
新たな類似データ
を生成
ST25
自局(C3)の
符号化パラメータ
を変更
ST26
符号化パラメータ
更新要求(s11)
ST24
通信データの
再出力要求(s12)
ST12

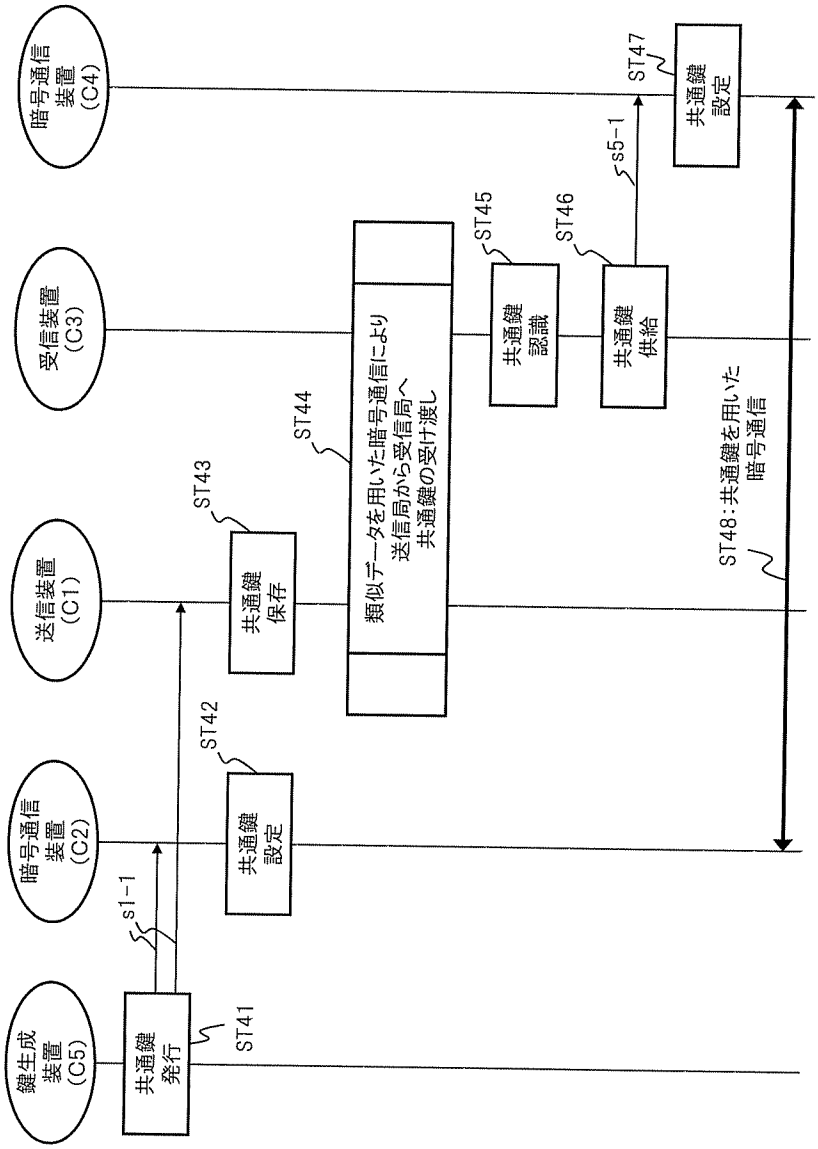
[図10]


送信装置
(C1)
ST31
類似データの
変更要求(s13)
を受信
No
Yes
ST32
新たな類似データ
を作成
ST33
符号化
パラメータ
更新要求(s11)
を受信
No
Yes
ST34
自局(C1)の
符号化パラメータ
を更新
ST35
通信データの
再出力要求(s12)
を受信
ST3
END

[図11]


102
C1
データ送信装置
B2
類似データ生成部
s13
s6
A2
暗号化部
s3
B3
通信部
s3
C3
データ受信装置
F2
類似データ生成部
s7
E2
暗号復号部
s3
F3
通信部
C5
鍵生成装置
s1-1
B4-1
鍵保持部
s1-1
A1
符号化部
s11
s2
s12
s4
s11/s13
s12
s13
符号復号部
E1
s5-1
s1-1
C2
暗号通信装置
C4
暗号通信装置

[図12]


暗号通信装置(C4)
受信装置(C3)
送信装置(C1)
暗号通信装置(C2)
鍵生成装置(C5)
共通鍵発行
共通鍵設定
共通鍵保存
類似データを用いた暗号通信により送信局から受信局へ共通鍵の受け渡し
共通鍵認識
共通鍵供給
共通鍵設定
ST41
ST42
ST43
ST44
ST45
ST46
ST47
s1-1
s5-1
ST48:共通鍵を用いた暗号通信

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/062929

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

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-538504 A (RSA Security Inc.), 12 November, 2002 (12.11.02), Par. Nos. [0033], [0054] to [0060]; Fig. 1 & US 2002/0029341 A1 & WO 2000/051244 A1	1,7,13,16, 21,22 2-6,8-12,14, 15,17-20
Y	JP 2004-187197 A (the Doshisha), 02 July, 2004 (02.07.04), Par. No. [0031] (Family: none)	2-6,8-12,14, 15,17-20
Y	WO 2006/038653 A1 (Matsushita Electric Industrial Co., Ltd.), 13 April, 2006 (13.04.06), Par. No. [0045] & JP 2006-109270 A & EP 1796299 A1 & CN 101036333 A	3-6,9-12,14, 15,18-20

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
14 October, 2008 (14.10.08)	21 October, 2008 (21.10.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/062929

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Feng Hao, Ross Anderson, John Daugman, Combining cryptography with biometrics effectively, UCAM-CL-TR-640, 2005.07, <URL: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-table.html>	4-6,10-12, 14,15,19,20
Y	Satoshi NAKAYAMA, Satoru YAMANO, "Undo no Kyoyu o Kagi to suru Kan'i · Anzen na Home Network", 2007 Nen The Institute of Electronics, Information and Communication Engineers Sogo Taikai Koen Ronbunshu, Tsushin 2, B-7-97, The Institute of Electronics, Information and Communication Engineers, 07 March, 2007 (07.03.07), page 187	5,6,11,12, 14,15,19,20
A	WO 2005/043805 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 12 May, 2005 (12.05.05), Abstract & JP 2007-510349 A & US 2008/0044027 A1	1-22
A	WO 2006/013798 A1 (Matsushita Electric Industrial Co., Ltd.), 09 February, 2006 (09.02.06), Abstract & EP 1764946 A1	1-22
A	JP 2001-77801 A (Advanced Mobile Telecommunications Security Technology Research Laboratories Co., Ltd.), 23 March, 2001 (23.03.01), Abstract; Fig. 1 (Family: none)	1-22
A	WO 2006/081122 A2 (INTERDIGITAL TECHNOLOGY CORP.), 03 August, 2006 (03.08.06), Abstract & US 2007/0058808 A1	1-22

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０６２９２９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

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

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

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2002-538504 A (アールエスエイ　セキュリティー　インコーポレーテッド) 2002.11.12, 【0033】, 【0054】-【0060】, 図１ & US 2002/0029341 A1 & WO 2000/051244 A1	1, 7, 13, 16, 21, 22
Y		2-6, 8-12, 14, 15, 17-20
Y	JP 2004-187197 A (学校法人同志社) 2004.07.02, 【0031】 (ファミリーなし)	2-6, 8-12, 14, 15, 17-20

☑　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	国際調査報告の発送日
１４．１０．２００８	２１．１０．２００８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３３６５
速水　雄太
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	関連する請求の範囲の番号
Y	WO 2006/038653 A1 (松下電器産業株式会社) 2006.04.13, [0045] & JP 2006-109270 A & EP 1796299 A1 & CN 101036333 A	3-6,9-12, 14,15,18-20
Y	Feng Hao, Ross Anderson, John Daugman, Combining cryptography with biometrics effectively, UCAM-CL-TR-640, 2005.07, <URL: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-table.html>	4-6,10-12, 14,15,19,20
Y	中山悟志，山野悟，運動の共有を鍵とする簡易・安全なホームネットワーク，２００７年電子情報通信学会総合大会講演論文集，通信２，Ｂ－７－９７，社団法人電子情報通信学会，2007.03.07，第１８７頁	5,6,11,12, 14,15,19,20
A	WO 2005/043805 A1 (KONINKLIJKE PHILIPS ELECTRONICS N.V.) 2005.05.12, Abstract & JP 2007-510349 A & US 2008/0044027 A1	1-22
A	WO 2006/013798 A1 (松下電器産業株式会社) 2006.02.09, 要約 & EP 1764946 A1	1-22
A	JP 2001-77801 A (株式会社高度移動通信セキュリティ技術研究所) 2001.03.23, 要約, 図１（ファミリーなし）	1-22
A	WO 2006/081122 A2 (INTERDIGITAL TECHNOLOGY CORPORATION) 2006.08.03, Abstract & US 2007/0058808 A1	1-22