(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
2017 年 9 月 14 日(14.09.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/154484 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
H04L 9/10 (2006.01)

(21) 国際出願番号: PCT/JP2017/005311

(22) 国際出願日: 2017 年 2 月 14 日(14.02.2017)

(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 2016-048244 2016 年 3 月 11 日(11.03.2016) JP

(71) 出願人: 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 佐藤　雅幸(SATOU Masayuki); 〒1088001 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: 加藤　卓士(KATO Takashi); 〒1620818 東京都新宿区築地町４　神楽坂テクノス５Ｆ Tokyo (JP).

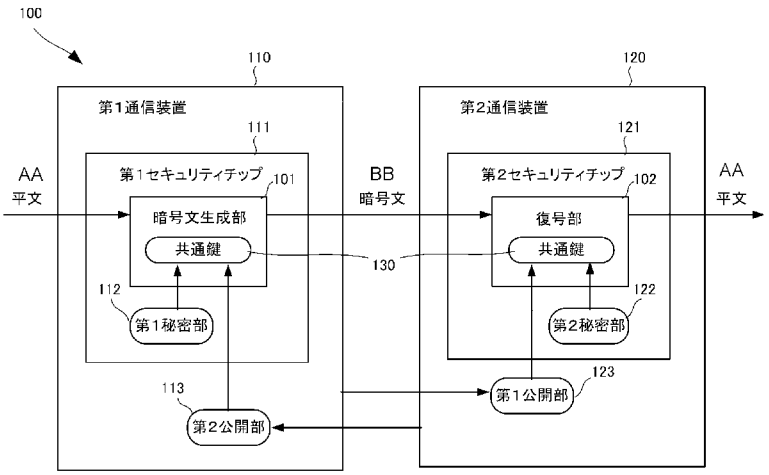
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: ENCRYPTED COMMUNICATION SYSTEM, ENCRYPTED COMMUNICATION METHOD, SECURITY CHIP, COMMUNICATION DEVICE AND CONTROL METHOD AND CONTROL PROGRAM FOR SAME

(54) 発明の名称 : 暗号通信システム、暗号通信方法、セキュリティチップ、通信装置およびその制御方法と制御プログラム



101 Encrypted text generating unit
102 Decrypting unit
110 First communication device
111 First security chip
112 First secret portion
113 Second public portion
120 Second communication device
121 Second security chip
122 Second secret portion
123 First public portion
130 Common key
AA Plaintext
BB Encrypted text

(57) **Abstract**: The present invention relates to an encrypted communication system with which confidentiality of communication information is enhanced by preventing leakage of a common key. This encrypted communication system employs a group comprising a first secret portion and a first public portion, and a group comprising a second secret portion and a second public portion, in a Key Predistribution System (KPS), and is provided with: an encrypted text generating unit which, in a first security chip (TMP) of a first communication device, uses the second public portion which has been transmitted from a second communication device constituting a communication partner, to generate a common key by means of the first secret portion held in the first security chip, and which, in the first security chip, generates encrypted text by encrypting plaintext on the basis of the common key; and a decrypting unit which, in a second security chip of the second communication device, uses the first public portion which has been transmitted from the first communication device constituting a communication partner, to generate the common key by means of the second secret portion held in the second security chip, and which, in the second security chip, decrypts the encrypted text, received from the first communication device, on the basis of the common key to generate plaintext.

(57) 要約:

[続葉有]

WO 2017/154484 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

本発明は共通鍵の漏洩を防いで通信情報の秘匿性を高める暗号通信システムに関する。暗号通信システムは、暗号鍵事前配布方式（ＫＰＳ)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信システムであって、第１通信装置の第１セキュリティチップ（ＴＭＰ)において、通信相手である第２通信装置から伝送された第２公開部を用いて第１セキュリティチップに保持された第１秘密部により共通鍵を生成し、第１セキュリティチップにおいて共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成部と、第２通信装置の第２セキュリティチップにおいて、通信相手である第１通信装置から伝送された第１公開部を用いて第２セキュリティチップに保持された第２秘密部により共通鍵を生成し、第２セキュリティチップにおいて共通鍵に基づいて、第１通信装置から受信した暗号文を復号して平文を生成する復号部と、を備える。

明　細　書

発明の名称 ：

暗号通信システム、暗号通信方法、セキュリティチップ、通信装置およびその制御方法と制御プログラム

技術分野

[0001]　本発明は、暗号通信システム、暗号通信方法、セキュリティチップ、通信装置およびその制御方法と制御プログラムに関する。

背景技術

[0002]　上記技術分野において、特許文献１には、ＴＰＭ(Trusted Platform Module)に公開鍵とその公開鍵に対応する秘密鍵を埋め込んで、情報が不用意に漏洩することのない技術が開示されている。また、非特許文献１の１３頁には、データを保護するため共通鍵をＴＰＭ内の公開鍵で暗号化（wrapping)し、復号（unwrapping)のための秘密鍵をＴＰＭ内に保管する技術が提案されている。

先行技術文献

特許文献

[0003] 特許文献1：特開２００８－３５４４９号公報

非特許文献

[0004] 非特許文献1：「ＴＰＭを活用したセキュリティ最前線(The security frontier levelaged by TPM)」、社団法人　電子情報産業協会(Japan Electronics and Information Technology Industries Association)　ＴＣＧ専門委員会、2007/10/3、http://home.jeita.or.jp/is/committee/infopolicy/tcg/d20071003.pdf

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、上記文献に記載の技術では、共通鍵による暗号化や復号時

に共通鍵がＴＰＭの外で使用される、あるいは、ＴＰＭ内に生成された共通鍵が常駐することにより、共通鍵の漏洩を防ぐことができなかった。

[0006] 本発明の目的は、上述の課題を解決する技術を提供することにある。

課題を解決するための手段

[0007] 上記目的を達成するため、本発明に係る暗号通信システムは、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信システムであって、

第１通信装置の第１セキュリティチップ（ＴＭＰ:Trusted Platform Module)において、通信相手である第２通信装置から伝送された前記第２公開部を用いて前記第１セキュリティチップに保持された前記第１秘密部により共通鍵を生成し、前記第１セキュリティチップにおいて該共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成手段と、

前記第２通信装置の第２セキュリティチップにおいて、通信相手である前記第１通信装置から伝送された前記第１公開部を用いて前記第２セキュリティチップに保持された前記第２秘密部により共通鍵を生成し、前記第２セキュリティチップにおいて該共通鍵に基づいて、前記第１通信装置から受信した前記暗号文を復号して平文を生成する復号手段と、

を備える。

[0008] 上記目的を達成するため、本発明に係る暗号通信方法は、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信方法であって、

第１通信装置の第１セキュリティチップ（ＴＭＰ:Trusted Platform Module)において、通信相手である第２通信装置から伝送された前記第２公開部を用いて前記第１セキュリティチップに保持された前記第１秘密部により共通鍵を生成し、前記第１セキュリティチップにおいて該共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成ステップと、

前記第２通信装置の第２セキュリティチップにおいて、通信相手である前記第１通信装置から伝送された前記第１公開部を用いて前記第２セキュリティチップに保持された前記第２秘密部により共通鍵を生成し、前記第２セキュリティチップにおいて該共通鍵に基づいて、前記第１通信装置から受信した前記暗号文を復号して平文を生成する復号ステップと、

を含む。

[0009] 上記目的を達成するため、本発明に係る通信装置は、

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置であって、

前記セキュリティチップが、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成手段と、

該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成手段と、

を備える。

[0010] 上記目的を達成するため、本発明に係る通信装置の制御方法は、

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成ステップと、

を含む。

[0011] 上記目的を達成するため、本発明に係る通信装置の制御プログラムは、

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御プログラムであって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成ステップと、

をコンピュータに実行させる。

[0012] 上記目的を達成するため、本発明に係る通信装置は、

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置であって、

前記セキュリティチップが、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成手段と、

該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号手段と、

を備える。

[0013] 上記目的を達成するため、本発明に係る通信装置の制御方法は、

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密

部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号ステップと、

を含む。

[0014] 上記目的を達成するため、本発明に係る通信装置の制御プログラムは、

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号ステップと、

をコンピュータに実行させる。

[0015] 上記目的を達成するため、本発明に係るセキュリティチップは、

通信装置が有するセキュリティチップ（ＴＭＰ:Trusted Platform Module)であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

前記保持された秘密部と通信相手から伝送された前記暗号鍵事前配布方式における公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

平文と前記通信相手から伝送された公開部とが添付された暗号化コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記平文を暗号化して暗号文を生成する暗号文生成手段と、

を備える。

[0016] 上記目的を達成するため、本発明に係るセキュリティチップは、

通信装置が有するセキュリティチップ（ＴＭＰ:Trusted Platform Module）であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

前記保持された秘密部と通信相手から伝送された前記暗号鍵事前配布方式における公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記暗号文を復号して平文を生成する復号手段、

を備える。

発明の効果

[0017] 本発明によれば、共通鍵の漏洩を防いで、通信情報の秘匿性を高めることができる。

図面の簡単な説明

[0018] [図1]本発明の第１実施形態に係る暗号通信システムの構成を示すブロック図である。

[図2A]本発明の第２実施形態に係る暗号通信システムの運用準備処理の動作手順を示すシーケンス図である。

[図2B]本発明の第２実施形態に係る暗号通信システムの暗号化処理の動作手順を示すシーケンス図である。

[図2C]本発明の第２実施形態に係る暗号通信システムの復号処理の動作手順を示すシーケンス図である。

[図3A]本発明の第２実施形態に係る暗号通信システムの概略構成を示すブロック図である。

[図3B]本発明の第２実施形態に係る通信装置の概略構成を示すブロック図である。

[図3C]本発明の第２実施形態に係る通信装置のソフトウェアレイヤ構成を示すブロック図である。

[図4A]本発明の第２実施形態に係る通信装置のハードウェア構成を示すブロック図である。

[図4B]本発明の第２実施形態に係る通信装置の運用準備処理の手順を示すフローチャートである。

[図4C]本発明の第２実施形態に係る通信装置の暗号文送信処理の手順を示すフローチャートである。

[図4D]本発明の第２実施形態に係る通信装置の平文復号処理の手順を示すフローチャートである。

[図5A]本発明の第２実施形態に係るセキュリティチップ（ＴＭＰ）のハードウェア構成を示すブロック図である。

[図5B]本発明の第２実施形態に係るセキュリティチップ（ＴＭＰ）の秘密部埋込処理の手順を示すフローチャートである。

[図5C]本発明の第２実施形態に係るセキュリティチップ（ＴＭＰ）の暗号化処理の手順を示すフローチャートである。

[図5D]本発明の第２実施形態に係るセキュリティチップ（ＴＭＰ）の復号処理の手順を示すフローチャートである。

[図6A]前提技術に係る暗号通信システムの暗号化処理の動作手順を示すシーケンス図である。

[図6B]前提技術に係る暗号通信システムの復号処理の動作手順を示すシーケンス図である。

[図6C]前提技術に係るセキュリティチップ（ＴＭＰ）のハードウェア構成を示すブロック図である。

[図6D]前提技術に係る暗号鍵事前配布方式（ＫＰＳ）のアルゴリズムの一例を示す図である。

[図7A]本発明の第３実施形態に係る暗号通信システムの運用準備処理の動作手順を示すシーケンス図である。

[図7B]本発明の第３実施形態に係る暗号通信システムの暗号化処理の動作手順を示すシーケンス図である。

[図7C]本発明の第３実施形態に係る暗号通信システムの復号処理の動作手順を示すシーケンス図である。

[図8A]本発明の第３実施形態に係る通信装置のハードウェア構成を示すブロック図である。

[図8B]本発明の第３実施形態に係る通信装置の運用準備処理の手順を示すフローチャートである。

[図9A]本発明の第３実施形態に係るセキュリティチップ（ＴＭＰ）のハードウェア構成を示すブロック図である。

[図9B]本発明の第３実施形態に係るセキュリティチップ（ＴＭＰ）の秘密部埋込処理の手順を示すフローチャートである。

[図10]本発明の第４実施形態に係る暗号通信システムの運用準備処理の動作手順を示すシーケンス図である。

[図11A]本発明の第４実施形態に係る通信装置に記憶される公開情報テーブルの構成を示す図である。

[図11B]本発明の第４実施形態に係る通信装置の運用準備処理の手順を示すフローチャートである。

[図11C]本発明の第４実施形態に係る通信装置の暗号文送信処理の手順を示すフローチャートである。

[図11D]本発明の第４実施形態に係る通信装置の平文復号処理の手順を示すフローチャートである。

[図12]本発明の第５実施形態に係る暗号通信システムのアプリケーションのダウンロード処理の動作手順を示すシーケンス図である。

発明を実施するための形態

[0019] 以下に、図面を参照して、本発明の実施の形態について例示的に詳しく説明する。ただし、以下の実施の形態に記載されている構成要素は単なる例示であり、本発明の技術範囲をそれらのみに限定する趣旨のものではない。

[0020] ［第１実施形態］

本発明の第１実施形態としての暗号通信システム１００について、図１を用いて説明する。暗号通信システム１００は、暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる通信装置間で暗号通信を行なうシステムである。

[0021] 図１に示すように、暗号通信システム１００は、暗号文生成部１０１と、復号部１０２と、を含む。暗号文生成部１０１は、第１通信装置１１０の第１セキュリティチップ（ＴＭＰ:Trusted Platform Module)１１１において、通信相手である第２通信装置１２０から伝送された第２公開部１１３を用いて第１セキュリティチップ１１１に保持された第１秘密部１１２により共通鍵１３０を生成し、第１セキュリティチップ１１１において共通鍵１３０に基づいて平文を暗号化して暗号文を生成する。復号部１０２は、第２通信装置１２０の第２セキュリティチップ１２１において、通信相手である第１通信装置１１０から伝送された第１公開部１２３を用いて第２セキュリティチップ１２１に保持された第２秘密部１２２により共通鍵１３０を生成し、第２セキュリティチップ１２１において共通鍵１３０に基づいて、第１通信装置１１０から受信した暗号文を復号して平文を生成する。 本実施形態によれば、第１通信装置では暗号化時にＴＰＭ内で第１秘密部および第２公開部から共通鍵を生成して、ＴＰＭ内で暗号化を行ない、第２通信装置では復号時にＴＰＭ内で第２秘密部および第１公開部から共通鍵を生成して、ＴＰＭ内で復号を行なうことで、共通鍵の漏洩を防いで、通信情報の秘匿性を高めることができる。

[0022] ［第２実施形態］

次に、本発明の第２実施形態に係る暗号通信システムについて説明する。本実施形態に係る暗号通信システムは、配布される暗号鍵事前配布方式における秘密部をＴＰＭに埋め込んで公開部を通信相手に伝送する。そして、暗号化や復号時にＴＰＭ内で共通鍵を生成して、ＴＰＭ内で暗号化や復号を行ない、終了後には共通鍵を破棄する。

[0023] 《前提技術》

まず、図６Ａ～図６Ｄを参照して、前提技術の構成および動作を簡単に説明する。

[0024] （暗号化処理シーケンス）

図６Ａは、前提技術に係る暗号通信システム６００の暗号化処理の動作手順を示すシーケンス図である。

[0025] 暗号側装置６１０の暗号側ＣＰＵ６１１は、ステップＳ６１１において、暗号側ＴＰＭ６１２に対して共通鍵のロードを要求する。暗号側装置６１０の暗号側ＴＰＭ６１２は、ステップＳ６１３において、共通鍵を暗号側ＣＰＵ６１１に渡す。

[0026] この時点で、共通鍵は暗号側ＣＰＵ６１１に公開されたことになる。暗号側ＣＰＵ６１１は、ステップＳ６１５において、ロードした共通鍵により平文メッセージを暗号化する。そして、暗号側ＣＰＵ６１１は、ステップＳ６１７において、暗号化されたメッセージを復号側装置６２０の復号側ＣＰＵ６２１に送信する。暗号側ＣＰＵ６１１は、ステップＳ６１９において、ロードした共通鍵を破棄する。この間（図６Ａの６０１参照）、共通鍵は暗号側ＣＰＵ６１１に生存し続けるので、共通鍵の漏洩確率が増大する。

[0027] （復号処理シーケンス）

図６Ｂは、前提技術に係る暗号通信システム６００の復号処理の動作手順を示すシーケンス図である。

[0028] 暗号側装置６１０の暗号側ＣＰＵ６１１は、上記ステップＳ６１７において、暗号化されたメッセージを復号側装置６２０の復号側ＣＰＵ６２１に送信する。

[0029] 復号側装置６２０の復号側ＣＰＵ６２１は、暗号化されたメッセージを受信して、ステップＳ６２１において、復号側ＴＰＭ６２２に対して共通鍵のロードを要求する。復号側装置６２０の復号側ＴＰＭ６２２は、ステップＳ６２３において、共通鍵を復号側ＣＰＵ６２１に渡す。

[0030] この時点で、共通鍵は復号側ＣＰＵ６２１に公開されたことになる。復号側ＣＰＵ６２１は、ステップＳ６２５において、ロードした共通鍵により暗号文メッセージを復号する。そして、復号側ＣＰＵ６２１は、ステップＳ６２７において、ロードした共通鍵を破棄する。この間（図６Ｂの６０２参照）、共通鍵は復号側ＣＰＵ６２１に生存し続けるので、共通鍵の漏洩確率が増大する。

[0031] （セキュリティチップの構成）

図６Ｃは、前提技術に係るセキュリティチップ（ＴＭＰ）６３０／６４０のハードウェア構成を示すブロック図である。

[0032] 図６Ｃは、ＴＣＧ(Trusted Computing Group)によるＴＰＭv1.2仕様の構成６３０と、ＴＰＭv2.0仕様の構成６４０と、である。なお、本実施形態においては、かかる構成にさらに、ＫＰＳ秘密部の不揮発メモリへの保持機能と、暗号化コマンドEncryptによる共通鍵生成および暗号化機能と、復号コマンドDecryptによる共通鍵生成および復号機能と、を付加している。

[0033] （暗号鍵事前配布方式のアルゴリズム例）

図６Ｄは、前提技術に係る暗号鍵事前配布方式（ＫＰＳ）のアルゴリズム６５０の一例を示す図である。なお、図６Ｄに示した暗号鍵事前配布方式（ＫＰＳ）のアルゴリズム６５０はBlomアルゴリズムと呼ばれる一例であり、本実施形態で使用可能な暗号鍵事前配布方式（ＫＰＳ）のアルゴリズムは図６Ｄに限定されない。

[0034] 図６Ｄの上半分（理論）は、Blomアルゴリズムに基づいて、（ＫＰＳ公開部，ＫＰＳ秘密部）との多数の組が生成されることを証明するものである。すなわち、暗号鍵事前配布方式（ＫＰＳ）のアルゴリズム６５０においては、ＫＳＰ公開部に対応してＫＰＳ秘密部が算出され、このＫＳＰ公開部を通

信先に伝送することによって、送信元と送信先において同じ共通鍵が算出されるものである。

[0035] 図６Ｄの下半分（具体例）には、簡単な具体的値に従ってBlomアルゴリズムに基づいて、上記理論が正しいことが示されている。ここでは、例えば、（γu=12，γv=7，γw=1）６５１が装置Ｕ，Ｖ，ＷのＫＰＳ公開部（公開値）である。このＫＰＳ公開部に対応して、ＫＰＳ秘密部（秘密値）が生成される。図６Ｄにおいては、（αu，βu)＝(７，１４）、(αv，βv)＝(６，４）、(αw，βw)＝(１５，９）、がＫＰＳ秘密部（秘密値）である。かかるＫＰＳ秘密部（秘密値）により、ｇu(x)＝７＋１４ｘ、ｇv(x)＝６＋４ｘ、ｇw(x)＝１５＋９ｘ、となり、互いの共通鍵はＵＶ間で“３”、ＵW間で“４”、ＶW間で“１０”となり、機密性が維持された暗号通信が可能となる。

[0036] 《本実施形態の説明》

以下、図２Ａ～図６Ｄにしたがって、本実施形態の構成および動作を詳細に説明する。

[0037] 《暗号通信システム》

まず、図２Ａ～図３Ａを参照して、本実施形態の暗号通信システム２００について説明する。

[0038] （運用準備処理シーケンス）

図２Ａは、本実施形態に係る暗号通信システム２００の運用準備処理の動作手順を示すシーケンス図である。

[0039] ＫＰＳの（公開部，秘密部）の組を配布する配布装置２３０は、ステップＳ２０１において、暗号側装置２１０（以下、Aliceとも略す）の暗号側ＣＰＵ２１１と、復号側装置２２０（以下、Bobとも略す）の復号側ＣＰＵ２２１と、にＫＰＳの（公開部，秘密部）の組を配布する。なお、図２Ａにおいては、配布装置２３０からＫＰＳの（公開部，秘密部）の組を配布する例を示したが、暗号側ＣＰＵ２１１または復号側ＣＰＵ２２１から公開部を送信し、秘密部を受領してもよい。

[0040] 暗号側ＣＰＵ２１１は、ステップＳ２１１において、暗号側ＴＰＭ２１２

に対して受領したＫＰＳ秘密部を埋め込んで秘密部保持するように指示する。暗号側ＴＰＭ２１２は、ステップＳ２１３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0041] また、暗号側ＣＰＵ２１１は、ステップＳ２１５において、受領したＫＰＳ公開部を復号側ＣＰＵ２２１に対して伝送し、復号側ＣＰＵ２２１から伝送された復号側のＫＰＳ公開部を受信する。そして、暗号側ＣＰＵ２１１は、ステップＳ２１７において、受信した復号側のＫＰＳ公開部を記憶する。

[0042] 一方、復号側ＣＰＵ２２１は、ステップＳ２２１において、復号側ＴＰＭ２２２に対して受領したＫＰＳ秘密部を埋め込むように指示する。復号側ＴＰＭ２２２は、ステップＳ２２３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0043] また、復号側ＣＰＵ２２１は、ステップＳ２２５において、受領したＫＰＳ公開部を暗号側ＣＰＵ２１１に対して伝送し、暗号側ＣＰＵ２１１から伝送された暗号側のＫＰＳ公開部を受信する。そして、復号側ＣＰＵ２２１は、ステップＳ２２７において、受信した暗号側のＫＰＳ公開部を記憶する。

[0044] （暗号化処理シーケンス）

図２Ｂは、本実施形態に係る暗号通信システム２００の暗号化処理の動作手順を示すシーケンス図である。

[0045] 暗号側ＣＰＵ２１１は、ステップＳ２３１において、記憶している復号側の公開情報（公開部）を読み出す。暗号側ＣＰＵ２１１は、ステップＳ２３３において、平文メッセージを取得して暗号側ＴＰＭ２１２にインプットする。すなわち、暗号側ＣＰＵ２１１は、ステップＳ２３５において、平文および復号側の公開情報を添付した暗号化コマンドEncrypt(平文，復号側の公開情報)を暗号側ＴＰＭ２１２に送信する。

[0046] 暗号側ＴＰＭ２１２は、受信した暗号化コマンドEncrypt(平文，復号側の公開情報)を解析して、“添付された復号側の公開情報を用いて暗号側ＴＰＭ２１２に保持された秘密部により共通鍵を生成し、その共通鍵で添付された平文を暗号化し、暗号文を暗号側ＣＰＵ２１１に返す”と判定する。そして

、暗号側ＴＰＭ２１２は、ステップＳ２３７において、暗号鍵事前配布方式（ＫＰＳ）に従い共通鍵を生成し、ステップＳ２３９において、この共通鍵で平文を暗号化して暗号文を生成する。

[0047] 暗号側ＴＰＭ２１２は、ステップＳ２４１において、共通鍵で暗号化した暗号文と暗号側ＴＰＭ２１２での処理のステータスとを添付した暗号化応答コマンドEncrypt(暗号文，ステータス）を暗号側ＣＰＵ２１１に返す。また、暗号側ＴＰＭ２１２は、ステップＳ２４３において、暗号化のために生成した共通鍵を破棄する。

[0048] 暗号側ＣＰＵ２１１は、ステップＳ２４５において、暗号側ＴＰＭ２１２から返された暗号文を復号側装置２２０の復号側ＣＰＵ２２１に伝送する。暗号文の伝送は、ステップＳ２４７において、暗号化されたメッセージとして復号側ＣＰＵ２２１に伝送される。

[0049] （復号処理シーケンス）

図２Ｃは、本実施形態に係る暗号通信システム２００の復号処理の動作手順を示すシーケンス図である。

[0050] 復号側ＣＰＵ２２１は、ステップＳ２５１において、暗号側ＣＰＵ２１１からステップＳ２４７で伝送された暗号化されたメッセージから暗号文を受信する。復号側ＣＰＵ２２１は、ステップＳ２５３において、記憶している暗号側の公開情報（公開部）を読み出す。復号側ＣＰＵ２２１は、ステップＳ２５５において、暗号文および暗号側の公開情報を添付した復号コマンドDecrypt(暗号文，暗号側の公開情報)を復号側ＴＰＭ２２２に送信する。

[0051] 復号側ＴＰＭ２２２は、受信した復号コマンドEncrypt(暗号文，暗号側の公開情報)を解析して、“添付された暗号側の公開情報を用いて復号側ＴＰＭ２２２に保持された秘密部により共通鍵を生成し、その共通鍵で添付された暗号文を復号し、平文を復号側ＣＰＵ２２１に返す”と判定する。そして、復号側ＴＰＭ２２２は、ステップＳ２５７において、暗号鍵事前配布方式（ＫＰＳ）に従い共通鍵を生成し、ステップＳ２５９において、この共通鍵で暗号文を復号して平文を生成する。

[0052] 復号側ＴＰＭ２２２は、ステップＳ２６１において、共通鍵で復号した平文と復号側ＴＰＭ２２２での処理のステータスとを添付した復号応答コマンドDecrypt(平文，ステータス）を復号側ＣＰＵ２２１に返す。また、復号側ＴＰＭ２２２は、ステップＳ２６３において、復号のために生成した共通鍵を破棄する。

[0053] （システム構成）

図３Ａは、本実施形態に係る暗号通信システム２００の概略構成を示すブロック図である。なお、図３Ａには、各通信装置における通信制御外の構成については省略している。

[0054] 暗号側装置２１０は、前述のＣＰＵ２１１とＴＰＭ２１２とを備える。ＣＰＵ２１１は、アプリケーション３１１と、暗号機能モジュール３１２と、Ｉ２Ｃ(Inter Integrated Circuit)３１３と、を有する。ここで、アプリケーション３１１は、主に、復号側装置２２０との通信を含むサービスを提供するソフトウェアからなる。また、暗号機能モジュール３１２は、アプリケーション３１１の動作に従って、ＴＰＭ２１２を使用して暗号化処理を行なうためのソフトウェアを含む。また、Ｉ２Ｃ３１３は、ＴＰＭ２１２とシリアルインタフェースで接続されるＧＰＩＯ(General Purpose Input/Output)として動作する。

[0055] また、復号側装置２２０は、前述のＣＰＵ２２１とＴＰＭ２２２とを備える。ＣＰＵ２２１は、アプリケーション３２１と、復号機能モジュール３２２と、Ｉ２Ｃ３２３と、を有する。ここで、アプリケーション３２１は、主に、暗号側装置２１０との通信を含むサービスを提供するソフトウェアからなる。また、復号機能モジュール３２２は、アプリケーション３２１の動作に従って、ＴＰＭ２２２を使用して復号処理を行なうためのソフトウェアを含む。また、Ｉ２Ｃ３２３は、ＴＰＭ２２２と２本の信号線（ＳＣＬ:Serial ClockとＳＤＡ:Serial Data）によるシリアルインタフェースで接続されるＧＰＩＯとして動作する。

[0056] 《通信装置》

図３Ｂ～図４Ｄを参照して、本実施形態の暗号側装置２１０および復号側装置２２０を含む通信装置について説明する。

[0057] （概略構成）

図３Ｂは、本実施形態に係る通信装置２１０／２２０の概略構成を示すブロック図である。なお、図３Ｂは、ＴＰＭ２１２／２２２を搭載する通信装置の一般的な構成を示し、本実施形態の通信装置は図３Ｂの構成に限定されない。

[0058] 通信装置２１０／２２０は、ＣＰＵ２１１／２２１と、ＲＯＭ３２０と、ＲＡＭ３４０と、制御部(Controller)３６０と、表示部(Display)３６１と、操作部(Keyboard)３６２と、を有する。なお、他の図示された構成については詳説を省略する。

[0059] ＣＰＵ２１１／２２１は、通信装置２１０／２２０を制御する中央処理装置である。ＲＯＭ３２０は、ブートプログラムや固定値を不揮発に保持する記憶部である。ＲＡＭ３４０は、ＣＰＵ２１１／２２１が書換可能な一時記憶として使用する記憶部である。制御部(Controller)３６０は、ＣＰＵバスとＩＯバスとを接続して周辺装置（ＩＤデバイス）を制御する。

[0060] （ソフトウェア構成）

図３Ｃは、本実施形態に係る通信装置２１０／２２０のソフトウェアレイヤ構成を示すブロック図である。なお、図３Ｃは、ＴＰＭ２１２／２２２を搭載する通信装置の一般的なソフトウェア構成を示し、本実施形態の通信装置は図３Ｃのソフトウェアレイヤ構成に限定されない。

[0061] 通信装置２１０／２２０のソフトウェア構成は、概略、図３Ａに示したように、アプリケーション(Application)３１１／３２１と、暗号機能モジュール３１２／復号機能モジュール３２２と、を含む。暗号機能モジュール３１２／復号機能モジュール３２２は、アプリケーション３１１／３２１とＴＳＰＩ(TCG Service Provider Interface)を介して接続するＴＳＰ(TCG Service Provider)を有する。また、暗号機能モジュール３１２／復号機能モジュール３２２は、ＴＳＰとＴＣＳＩ(TSS Core Services Interface)を介して接続

するＴＣＳ(TSS Core Services)を有する。また、暗号機能モジュール３１２／復号機能モジュール３２２は、ＴＣＳＩとＴＤＤＬＩ(TPM Device Driver Library Interface)を介して接続するＴＤＤＬ(TCG Device Driver Library)を有する。また、暗号機能モジュール３１２／復号機能モジュール３２２は、ＴＰＭ２１２／２２２を駆動制御するＴＤＤ(TPM Device Driver)を有する。

[0062] （ハードウェア構成）

図４Ａは、本実施形態に係る通信装置２１０／２２０のハードウェア構成を示すブロック図である。

[0063] 図４Ａで、ＣＰＵ２１１／２２１は演算制御用のプロセッサであり、プログラムを実行することで図３Ａ乃至図３Ｃの機能構成部を実現する。ＲＯＭ３２０は、初期データおよびプログラムなどの固定データおよびプログラムを記憶する。通信制御部４３０は、ネットワークを介してサーバや他の通信装置との通信を制御する。入出力インタフェース３６０は、表示部や操作部などの入出力を制御する。

[0064] ＲＡＭ３４０は、ＣＰＵ２１１／２２１が一時記憶のワークエリアとして使用するランダムアクセスメモリである。ＲＡＭ３４０には、本実施形態の実現に必要なデータを記憶する領域が確保されている。平文は、暗号側装置２１０の場合の暗号前の文である。変分からの暗号文は、暗号側装置２１０の場合に平文から本実施形態の暗号化処理により生成された暗号化後の文である。受信した暗号文は、復号側装置２２０の場合の暗号側装置２１０から伝送された暗号化された文である。暗号文から復号した平文は、復号側装置２２０の場合の本実施形態の復号処理により暗号文から復号された文である。送受信データは、通信制御部４３０を介してサーバや他の通信装置とやり取りするメッセージデータである。入出力データは、入出力インタフェース３６０を介して入出力デバイスとやり取りするデータである。

[0065] ストレージ４５０は、データベースや各種のパラメータ、あるいは本実施形態の実現に必要な以下のデータまたはプログラムが記憶されている。通信

相手の公開情報保持部４５１は、通信相手の通信装置から伝送され、暗号化または復号時に共有鍵を生成するために使用されるＫＰＳ公開部を保持する。ストレージ４５０には、以下のプログラムが保持される。通信装置制御プログラムは、通信装置２１０／２２０の全体を制御するプログラムである。ＫＰＳ秘密部埋込モジュールは、配布されたＫＰＳ秘密部をＴＭＰに埋め込むためのモジュールである。ＫＰＳ公開部伝送モジュールは、配布されたＫＰＳ公開部を通信相手の通信装置に伝送するためのモジュールである。なお、ＫＰＳ秘密部埋込モジュールとＫＰＳ公開部伝送モジュールとを、まとめて運用準備モジュールとしてもよい。暗号文送信モジュールは、ＴＰＭ内においてＫＰＳ秘密鍵および通信相手から伝送されたＫＰＳ公開鍵から共通鍵を生成して、平文をこの共通鍵で暗号化し、通信相手の通信装置に暗号文を送信するモジュールである。平文復号モジュールは、ＴＰＭ内においてＫＰＳ秘密鍵および通信相手から伝送されたＫＰＳ公開鍵から共通鍵を生成して、通信相手から受信した暗号文をこの共通鍵で復号し、元の平文を生成するモジュールである。

[0066] 入出力インタフェース３６０には、表示部３６１と、操作部３６２と、ＴＰＭ２１２／２２２と、が接続される。なお、ＴＰＭ２１２／２２２は、別のインタフェースにより接続されてもよい。

[0067] なお、図４ＡのＲＡＭ３４０やストレージ４５０には、通信装置２１０／２２０が有する汎用の機能や他の実現可能な機能に関連するプログラムやデータは図示されていない。

[0068] （運用準備処理手順）

図４Ｂは、本実施形態に係る通信装置２１０／２２０の運用準備処理の手順を示すフローチャートである。このフローチャートは、図４ＡのＣＰＵ２１１／２２１がＲＡＭ３４０を使用して実行し、図３Ａ～図３Ｃの機能構成部を実現する。なお、以下の通信装置２１０／２２０の処理手順は、通信装置２１０／２２０が暗号化および復号の両処理機能を備えたものとして説明するが、実際には、暗号側装置専用または復号側装置専用の装置もあり、こ

れらも含むものである。

[0069] 通信装置２１０／２２０は、ステップＳ４１１において、ＫＰＳにおける（公開部，秘密部）の組を取得する。なお、前述した如く、公開部に基づいて秘密部を取得してもよい。通信装置２１０／２２０は、ステップＳ４１３において、ＴＰＭに対してＫＰＳ秘密部の埋め込みを指示する。通信装置２１０／２２０は、ステップＳ４１５において、通信相手のＣＰＵに対してＫＰＳ公開部を伝送する。

[0070] 通信装置２１０／２２０は、ステップＳ４１７において、通信相手からのＫＰＳ公開部の受信を待って、ＫＰＳ公開部の受信があれば、ステップＳ４１９において、受信した通信相手のＫＰＳ公開部を記憶する。

[0071] （暗号文送信処理手順）

図４Ｃは、本実施形態に係る通信装置２１０／２２０の暗号文送信処理の手順を示すフローチャートである。このフローチャートは、図４ＡのＣＰＵ２１１／２２１がＲＡＭ３４０を使用して実行し、図３Ａ～図３Ｃの機能構成部を実現する。

[0072] 通信装置２１０／２２０は、ステップＳ４２１において、暗号化対象の平文メッセージがあるか否かを判定する。暗号化対象の平文メッセージがあれば、通信装置２１０／２２０は、ステップＳ４２３において、記憶していた送信先の公開情報（公開部）を読み出す。そして、通信装置２１０／２２０は、ステップＳ４２５において、平文と公開情報とを添付した暗号化コマンドEncryptをＴＰＭに送付する。

[0073] 通信装置２１０／２２０は、ステップＳ４２７において、ＴＰＭからの暗号文の返信を待って、ＴＰＭからの暗号文の返信があれば、ステップＳ４２９において、暗号文を送信先に送付する。

[0074] （平文復号処理手順）

図４Ｄは、本２実施形態に係る通信装置２１０／２２０の平文復号処理の手順を示すフローチャートである。このフローチャートは、図４ＡのＣＰＵ２１１／２２１がＲＡＭ３４０を使用して実行し、図３Ａ～図３Ｃの機能構

成部を実現する。

[0075] 通信装置２１０／２２０は、ステップＳ４３１において、復号対象の暗号文メッセージがあるか否かを判定する。復号対象の暗号文メッセージがあれば、通信装置２１０／２２０は、ステップＳ４３３において、記憶していた送信元の公開情報（公開部）を読み出す。そして、通信装置２１０／２２０は、ステップＳ４３５において、暗号文と公開情報とを添付した復号コマンドDecryptをＴＰＭに送付する。

[0076] 通信装置２１０／２２０は、ステップＳ４３７において、ＴＰＭからの平文の返信を待って、ＴＰＭからの平文の返信があれば、ステップＳ４３９において、平文を出力する。

[0077] 《セキュリティチップ》

図５Ａ～図５Ｄを参照して、本実施形態のセキュリティチップ（ＴＭＰ）２１２／２２２の構成および動作を説明する。

[0078] （ハードウェア構成）

図５Ａは、本実施形態に係るセキュリティチップ（ＴＭＰ）２１２／２２２のハードウェア構成を示すブロック図である。なお、図５Ａは、本実施形態のセキュリティチップ（ＴＭＰ）２１２／２２２の構成例でありこれに限定されない。すなわち、さらに種々の機能が追加可能である。

[0079] セキュリティチップ（ＴＭＰ）２１２／２２２は、ＴＭＰ用ＣＰＵ５１０と、不揮発メモリ５２０と、入出力インタフェース（Ｉ／Ｏ）５３０と、ＲＡＭ５４０と、プログラム５５０と、を備える。

[0080] ＴＭＰ用ＣＰＵ５１０は、ＴＭＰ全体を制御して各機能を実現する。不揮発メモリ５２０は電源なしでも記憶内容を維持するメモリであり、ＫＰＳ秘密部５２１の記憶領域が確保されている。なお、ＫＰＳ秘密部５２１の記憶領域は、暗号化や復号時に読み出し可能であれば固定であっても変化してもよい。入出力インタフェース（Ｉ／Ｏ）５３０は、ＴＭＰと装置のＣＰＵ２１１／２２１とを接続するためのインタフェースである。ＲＡＭ５４０は、ＴＭＰ用ＣＰＵ５１０が一時記憶のために使用する記憶部である。プログラ

ム５５０は、ＴＭＰが実現する機能に対応するプログラムを保持し、本実施形態においては、ＫＰＳ演算モジュール５５１と、秘密部埋込モジュール５５２と、暗号化モジュールおよび復号モジュール５５３と、を保持する。

[0081] ＫＰＳ演算モジュール５５１は、暗号化コマンドや復号コマンドを受信して、通信相手の公開部を用いて秘密部により共通鍵を生成するモジュールである。秘密部埋込モジュール５５２は、装置ＣＰＵからの指示に従ってＫＰＳ秘密部を不揮発メモリに保持するモジュールである。暗号化モジュールおよび復号モジュール５５３は、ＫＰＳ演算モジュール５５１により生成された共通鍵を用いて、平文を暗号文に、暗号文を平文にするモジュールである。

[0082] なお、上記参照符号を付して説明した以外の構成要素は、ＴＰＭが一般に備える機能を示すブロックであり、ここでは説明を省略する。

[0083] （秘密部埋込処理手順）

図５Ｂは、本実施形態に係るセキュリティチップ（ＴＭＰ）２１２／２２２の秘密部埋込処理の手順を示すフローチャートである。このフローチャートは、図５ＡのＴＭＰ用ＣＰＵ５１０がＲＡＭ５４０を用いて実行し、図５Ａの機能構成部を実現する。なお、以下のセキュリティチップ（ＴＭＰ）２１２／２２２の処理手順は、セキュリティチップ（ＴＭＰ）２１２／２２２が暗号化および復号の両処理機能を備えた通信装置で使用されているとして説明するが、実際には、暗号側装置専用または復号側装置専用のセキュリティチップ（ＴＭＰ）もあり、これらも含むものである。

[0084] セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５１１において、ＫＰＳ秘密部の埋込コマンドの受信を待つ。ＫＰＳ秘密部の埋込コマンドを受信した場合、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５１３において、埋込コマンドのからＫＰＳ秘密部を取得する。そして、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５１５において、取得されたＫＰＳ秘密部を不揮発メモリに保存する。

[0085] （暗号化処理手順）

図５Ｃは、本実施形態に係るセキュリティチップ（ＴＭＰ）２１２／２２２の暗号化処理の手順を示すフローチャートである。このフローチャートは、図５ＡのＴＭＰ用ＣＰＵ５１０がＲＡＭ５４０を用いて実行し、図５Ａの機能構成部を実現する。

[0086] セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５２１において、暗号化コマンドEncryptの受信を待つ。暗号化コマンドEncryptの受信があると、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５２３において、暗号化コマンドから添付された平文と公開情報（公開部）とを取得する。そして、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５２５において、取得した公開情報を用いてＴＭＰ内のＫＳＰ秘密部に基づき共通鍵を算出する。

[0087] セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５２７において、算出した共通鍵により取得した平文を暗号化する。セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５２９において、算出した共通鍵を破棄する。そして、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５３１において、暗号文とステータスとを添付して装置ＣＰＵからの暗号化コマンドに返信する。

[0088] （復号処理の手順）

図５Ｄは、本実施形態に係るセキュリティチップ（ＴＭＰ）２１２／２２２の復号処理の手順を示すフローチャートである。このフローチャートは、図５ＡのＴＭＰ用ＣＰＵ５１０がＲＡＭ５４０を用いて実行し、図５Ａの機能構成部を実現する。

[0089] セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５４１において、復号コマンドDecryptの受信を待つ。復号コマンドDecryptの受信があると、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５４３において、復号コマンドから添付された暗号文と公開情報（公開部）とを取得する。そして、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５４５において、取得した公開情報を用いてＴＭＰ内のＫＳＰ秘密部に

基づき共通鍵を算出する。

[0090] セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５４７において、算出した共通鍵により取得した暗号文を復号する。セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５４９において、算出した共通鍵を破棄する。そして、セキュリティチップ（ＴＭＰ）２１２／２２２は、ステップＳ５５１において、平文とステータスとを添付して装置ＣＰＵからの復号コマンドに返信する。

[0091] 本発明によれば、暗号化や復号時にＴＰＭ内で共通鍵を生成して、ＴＰＭ内で暗号化や復号を行ない、終了後には共通鍵を破棄することにより、共通鍵の漏洩を防いで、通信情報の秘匿性を高めることができる。

[0092] ［第３実施形態］

次に、本発明の第３実施形態に係る暗号通信システムについて説明する。本実施形態に係る暗号通信システムは、上記第２実施形態と比べると、さらに、共通鍵暗号のＣＢＣモード(Cipher Block Chaining Mode)、あるいは、ＣＦＢモード(Cipher Feedback Mode)で使用される初期ベクタ(ＩＶ：Initialization Vector)の共有のために、初期ベクタ用のＫＰＳの秘密アルゴリズム部分をＴＰＭ内に隠ぺいし、公開部は自由に公開する点で異なる。その他の構成および動作は、第２実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

[0093] 《暗号通信システム》

図７Ａ～図７Ｃを参照して、本実施形態の暗号通信システム７００の構成および動作について説明する。

[0094] （運用準備処理シーケンス）

図７Ａは、本実施形態に係る暗号通信システム７００の運用準備処理の動作手順を示すシーケンス図である。なお、図７Ａにおける各ステップは、図２ＡにおけるＫＰＳ公開部およびＫＰＳ秘密部を、初期値ベクタ（ＩＶ）の共有にまで拡張したものである。

[0095] 初期値ベクタ（ＩＶ）に対しても、ＫＰＳの（公開部，秘密部）の組を配

布する配布装置７３０は、ステップＳ７０１において、暗号側装置７１０の暗号側ＣＰＵ７１１と、復号側装置７２０の復号側ＣＰＵ７２１と、にＫＰＳの（公開部，秘密部）の組を配布する。なお、図７Ａにおいては、配布装置７３０からＫＰＳの（公開部，秘密部）の組を配布する例を示したが、暗号側ＣＰＵ７１１または復号側ＣＰＵ７２１から公開部を送信し、秘密部を受領してもよい。

[0096] 暗号側ＣＰＵ７１１は、ステップＳ７１１において、暗号側ＴＰＭ７１２に対して受領したＫＰＳ秘密部を埋め込むように指示する。暗号側ＴＰＭ７１２は、ステップＳ７１３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0097] また、暗号側ＣＰＵ７１１は、ステップＳ７１５において、受領したＫＰＳ公開部を復号側ＣＰＵ７２１に対して伝送し、復号側ＣＰＵ７２１から伝送された復号側のＫＰＳ公開部を受信する。そして、暗号側ＣＰＵ７１１は、ステップＳ７１７において、受信した復号側のＫＰＳ公開部を記憶する。

[0098] 一方、復号側ＣＰＵ７２１は、ステップＳ７２１において、復号側ＴＰＭ７２２に対して受領したＫＰＳ秘密部を埋め込むように指示する。復号側ＴＰＭ７２２は、ステップＳ７２３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0099] また、復号側ＣＰＵ７２１は、ステップＳ７２５において、受領したＫＰＳ公開部を暗号側ＣＰＵ７１１に対して伝送し、暗号側ＣＰＵ７１１から伝送された暗号側のＫＰＳ公開部を受信する。そして、復号側ＣＰＵ７２１は、ステップＳ７２７において、受信した暗号側のＫＰＳ公開部を記憶する。

[0100] （暗号化処理シーケンス）

図７Ｂは、本実施形態に係る暗号通信システム７００の暗号化処理の動作手順を示すシーケンス図である。なお、図７Ｂにおける各ステップは、図２ＢにおけるＫＰＳ公開部およびＫＰＳ秘密部を、初期値ベクタ（ＩＶ）の共有にまで拡張したものである。また、図７Ｂにおいて、図２Ｂと同様のステップには同じステップ番号を付している。

初期値ベクタ（ＩＶ）に対しても、暗号側ＣＰＵ７１１は、ステップＳ７３１において、記憶している復号側の公開情報（公開部）を読み出す。暗号側ＣＰＵ７１１は、ステップＳ７３３において、平文メッセージを取得して暗号側ＴＰＭ７１２にインプットする。すなわち、暗号側ＣＰＵ７１１は、ステップＳ７３５において、平文および復号側の公開情報を添付した暗号化コマンドEncrypt(平文，復号側の鍵用公開情報，復号側のIV用公開情報)を暗号側ＴＰＭ７１２に送信する。

[0101] 暗号側ＴＰＭ７１２は、受信した暗号化コマンドEncrypt(平文，復号側の鍵用公開情報，復号側のIV用公開情報)を解析して、“添付された復号側の鍵用公開情報およびIV用公開情報を用いて暗号側ＴＰＭ７１２に保持された秘密部により共通鍵を生成し、その共通鍵で添付された平文をブロックごとに繰り返し暗号化し、暗号文を暗号側ＣＰＵ７１１に返す”と判定する。そして、暗号側ＴＰＭ７１２は、ステップＳ７３７において、暗号鍵事前配布方式（ＫＰＳ）に従い共通鍵を生成し、ステップＳ７３９において、この共通鍵で平文を暗号化して暗号文を生成する。

[0102] 暗号側ＴＰＭ７１２は、ステップＳ２４１において、共通鍵で暗号化した暗号文と暗号側ＴＰＭ７１２での処理のステータスとを添付した暗号化応答コマンドEncrypt(暗号文，ステータス）を暗号側ＣＰＵ７１１に返す。また、暗号側ＴＰＭ７１２は、ステップＳ７４３において、暗号化のために生成した共通鍵を破棄する。

[0103] 暗号側ＣＰＵ７１１は、ステップＳ２４５において、暗号側ＴＰＭ７１２から返された暗号文を復号側装置７２０の復号側ＣＰＵ７２１に伝送する。暗号文の伝送は、ステップＳ２４７において、暗号化されたメッセージとして復号側ＣＰＵ７２１に伝送される。

[0104] （復号処理シーケンス）

図７Ｃは、本実施形態に係る暗号通信システム７００の復号処理の動作手順を示すシーケンス図である。なお、図７Ｃにおける各ステップは、図２ＢにおけるＫＰＳ公開部およびＫＰＳ秘密部を、初期値ベクタ（ＩＶ）の共有

にまで拡張したものである。また、図７Ｃにおいて、図２Ｃと同様のステップには同じステップ番号を付している。

復号側ＣＰＵ７２１は、ステップＳ２５１において、暗号側ＣＰＵ２１１からステップＳ２４７で伝送された暗号化されたメッセージから暗号文を受信する。復号側ＣＰＵ７２１は、ステップＳ７５３において、記憶している暗号側の公開情報（公開部）を読み出す。復号側ＣＰＵ７２１は、ステップＳ７５５において、暗号文および暗号側の公開情報を添付した復号コマンドDecrypt(暗号文，暗号側の鍵用公開情報，暗号側のIV用公開情報)を復号側ＴＰＭ７２２に送信する。

[0105] 復号側ＴＰＭ７２２は、受信した復号コマンドEncrypt(暗号文，暗号側の鍵用公開情報，暗号側のIV用公開情報)を解析して、“添付された暗号側の鍵用公開情報およびIV用公開情報を用いて復号側ＴＰＭ７２２に保持された秘密部により共通鍵を生成し、その共通鍵で添付された暗号文を復号し、平文を復号側ＣＰＵ７２１に返す”と判定する。そして、復号側ＴＰＭ７２２は、ステップＳ７５７において、暗号鍵事前配布方式（ＫＰＳ）に従い共通鍵を生成し、ステップＳ７５９において、この共通鍵で暗号文を復号して平文を生成する。

[0106] 復号側ＴＰＭ７２２は、ステップＳ２６１において、共通鍵で復号した平文と復号側ＴＰＭ２２２での処理のステータスとを添付した復号応答コマンドDecrypt(平文，ステータス）を復号側ＣＰＵ７２１に返す。また、復号側ＴＰＭ７２２は、ステップＳ７６３において、復号のために生成した共通鍵を破棄する。

[0107] 《通信装置》

図８Ａおよび図８Ｂを参照して、本実施形態の通信装置７１０／７２０の構成および動作について説明する。

[0108] （ハードウェア構成）

図８Ａは、本実施形態に係る通信装置７１０／７２０のハードウェア構成を示すブロック図である。なお、図８Ａにおいて、図４Ａと同様の構成要素

には同じ参照番号を付して、説明を省略する。

[0109] 図８Ａで、ＣＰＵ７１１／７２１は演算制御用のプロセッサであり、プログラムを実行することで図７Ａ乃至図７Ｃの機能構成部を実現する。

[0110] ストレージ８５０は、データベースや各種のパラメータ、あるいは本実施形態の実現に必要な以下のデータまたはプログラムが記憶されている。通信相手の鍵用公開情報保持部８５１は、通信相手の通信装置から伝送され、暗号化または復号時に共有鍵を生成するために使用される共通鍵生成用のＫＰＳ公開部を保持する。通信相手のIV用公開情報保持部８５２は、通信相手の通信装置から伝送され、暗号化または復号時に共有鍵を生成するために使用されるＩＶ生成用のＫＰＳ公開部を保持する。

[0111] 入出力インタフェース３６０には、ＴＰＭ７１２／７２２と、が接続される。なお、ＴＰＭ７１２／７２２は、別のインタフェースにより接続されてもよい。

[0112] なお、図８ＡのＲＡＭ３４０やストレージ８５０には、通信装置７１０／７２０が有する汎用の機能や他の実現可能な機能に関連するプログラムやデータは図示されていない。

（運用準備処理手順）

図８Ｂは、本実施形態に係る通信装置７１０／７２０の運用準備処理の手順を示すフローチャートである。このフローチャートは、図８ＡのＣＰＵ７１１／７２１がＲＡＭ３４０を使用して実行し、図７Ａ～図７Ｃの機能構成部を実現する。なお、以下の通信装置７１０／７２０の処理手順は、通信装置７１０／７２０が暗号化および復号の両処理機能を備えたものとして説明するが、実際には、暗号側装置専用または復号側装置専用の装置もあり、これらも含むものである。また、図８Ｂにおける各ステップは、図４ＢにおけるＫＰＳ公開部およびＫＰＳ秘密部を、初期値ベクタ（ＩＶ）の共有にまで拡張したものである。

[0113] 通信装置７１０／７２０は、ステップＳ８１１において、初期値ベクタ（ＩＶ）も含むＫＰＳにおける（公開部，秘密部）の組を取得する。なお、前

述した如く、公開部に基づいて秘密部を取得してもよい。通信装置７１０／７２０は、ステップＳ８１３において、ＴＰＭに対してＫＰＳ秘密部の埋め込みを指示する。通信装置７１０／７２０は、ステップＳ８１５において、通信相手のＣＰＵに対してＫＰＳ公開部を伝送する。

[0114] 通信装置７１０／７２０は、ステップＳ８１７において、通信相手からのＫＰＳ公開部の受信を待って、ＫＰＳ公開部の受信があれば、ステップＳ８１９において、受信した通信相手のＫＰＳ公開部を記憶する。

[0115] 《セキュリティチップ》

図９Ａおよび図９Ｂを参照して、本実施形態のセキュリティチップ（ＴＭＰ）７１２／７２２の構成および動作について説明する。

[0116] （ハードウェア構成）

図９Ａは、本実施形態に係るセキュリティチップ（ＴＭＰ）７１２／７２２のハードウェア構成を示すブロック図である。なお、図９Ａにおいて、図５Ａと同様な機能構成部には同じ参照番号を付して、重複する説明を省略する。

[0117] 不揮発メモリ９２０は、鍵用ＫＰＳ秘密部９２１とIV用ＫＰＳ秘密部９２２とを保持する。また、プログラム９５０は、ＴＭＰが実現する機能に対応するプログラムを保持し、本実施形態においては、ＫＰＳ演算モジュール９５１と、秘密部埋込モジュール９５２と、暗号化モジュールおよび復号モジュール９５３と、を保持する。

[0118] ＫＰＳ演算モジュール９５１は、暗号化コマンドや復号コマンドを受信して、通信相手の公開部を用いて秘密部により共通鍵およびＩＶを生成するモジュールである。秘密部埋込モジュール９５２は、装置ＣＰＵからの指示に従って共通鍵およびＩＶを生成するＫＰＳ秘密部を不揮発メモリに保持するモジュールである。暗号化モジュールおよび復号モジュール９５３は、ＫＰＳ演算モジュール９５１により生成された共通鍵およびＩＶを用いて、平文を暗号文に、暗号文を平文にするモジュールである。

[0119] （秘密部埋込処理手順）

図９Ｂは、本実施形態に係るセキュリティチップ（ＴＭＰ）７１２／７２２の秘密部埋込処理の手順を示すフローチャートである。このフローチャートは、図９ＡのＴＭＰ用ＣＰＵ５１０がＲＡＭ５４０を用いて実行し、図９Ａの機能構成部を実現する。なお、以下のセキュリティチップ（ＴＭＰ）７１２／７２２の処理手順は、セキュリティチップ（ＴＭＰ）７１２／７２２が暗号化および復号の両処理機能を備えた通信装置で使用されているとして説明するが、実際には、暗号側装置専用または復号側装置専用のセキュリティチップ（ＴＭＰ）もあり、これらも含むものである。また、図９Ａにおける各ステップは、図５ＢにおけるＫＰＳ公開部およびＫＰＳ秘密部を、初期値ベクタ（ＩＶ）の共有にまで拡張したものである。

[0120] セキュリティチップ（ＴＭＰ）７１２／７２２は、ステップＳ９１１において、初期値ベクタ（ＩＶ）も含むＫＰＳ秘密部の埋込コマンドの受信を待つ。ＫＰＳ秘密部の埋込コマンドを受信した場合、セキュリティチップ（ＴＭＰ）７１２／７２２は、ステップＳ９１３において、埋込コマンドのからＫＰＳ秘密部を取得する。そして、セキュリティチップ（ＴＭＰ）７１２／７２２は、ステップＳ９１５において、取得された共通鍵およびＩＶ用のＫＰＳ秘密部を不揮発メモリに保存する。

[0121] なお、本実施形態では説明しなかったが、２ブロック目以降の暗号化ないし復号に用いる初期ベクタは、ＣＢＣモード、ＣＦＢモードにより、ＴＰＭ内で更新するものとする。

[0122] 本実施形態によれば、さらに、共通鍵暗号のＣＢＣモード、あるいは、ＣＦＢモードで使用される初期ベクタ(ＩＶ）の漏洩を防いで、通信情報の秘匿性を高めることができる。

[0123] ［第４実施形態］

次に、本発明の第４実施形態に係る暗号通信システムについて説明する。本実施形態に係る暗号通信システムは、上記第２実施形態および第３実施形態と比べると、３つ以上の通信装置間で秘密部とお互いの公開部とから共通鍵あるいは初期化ベクタを生成する点で異なる。その他の構成および動作は

、第２実施形態または第３実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

[0124] （運用準備処理シーケンス）

図１０は、本実施形態に係る暗号通信システムの運用準備処理の動作手順を示すシーケンス図である。なお、図１０における各ステップは、図２ＡにおけるＫＰＳ公開部およびＫＰＳ秘密部を、３つ以上の通信装置間での互いの共有にまで拡張したものである。また、図１０においては、る配布装置２３０によるＫＰＳの（公開部，秘密部）の組を各通信装置のＣＰＵに配布するステップは、重複を避けるため図示していない。

[0125] 装置ＵのＣＰＵ１０１１は、ステップＳ１０１１において、装置ＵのＴＰＭ１０１２に対して受領したＫＰＳ秘密部を埋め込むように指示する。装置ＵのＴＰＭ１０１２は、ステップＳ１０１３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0126] また、装置ＵのＣＰＵ１０１１は、ステップＳ１０１５において、受領したＫＰＳ公開部を装置ＶのＣＰＵ１０２１に対して伝送し、装置ＶのＣＰＵ１０２１から伝送された装置ＶのＫＰＳ公開部を受信する。そして、装置ＵのＣＰＵ１０１１は、ステップＳ１０１７において、受信した装置ＶのＫＰＳ公開部を記憶する。

[0127] 一方、装置ＶのＣＰＵ１０２１は、ステップＳ１０３１において、装置ＶのＴＰＭ１０２２に対して受領したＫＰＳ秘密部を埋め込むように指示する。装置ＶのＴＰＭ１０２２は、ステップＳ１０３３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0128] また、装置ＶのＣＰＵ１０２１は、ステップＳ１０３５において、受領したＫＰＳ公開部を装置ＵのＣＰＵ１０１１に対して伝送し、装置ＵのＣＰＵ１０１１から伝送された装置ＵのＫＰＳ公開部を受信する。そして、装置ＶのＣＰＵ１０２１は、ステップＳ１０３７において、受信した装置ＵのＫＰＳ公開部を記憶する。

[0129] また、装置ＶのＣＰＵ１０２１は、ステップＳ１０３９において、受領し

たＫＰＳ公開部を装置WのＣＰＵ１０３１に対して伝送し、装置WのＣＰＵ１０３１から伝送された装置WのＫＰＳ公開部を受信する。そして、装置ＶのＣＰＵ１０２１は、ステップＳ１０４１において、受信した装置WのＫＰＳ公開部を記憶する。

[0130] 一方、装置WのＣＰＵ１０３１は、ステップＳ１０５１において、装置WのＴＰＭ１０３２に対して受領したＫＰＳ秘密部を埋め込むように指示する。装置WのＴＰＭ１０３２は、ステップＳ１０５３において、ＫＰＳ秘密部をセキュアに不揮発メモリの所定位置に保持する。

[0131] また、装置WのＣＰＵ１０３１は、ステップＳ１０５５において、受領したＫＰＳ公開部を装置ＶのＣＰＵ１０２１に対して伝送し、装置ＶのＣＰＵ１０２１から伝送された装置ＶのＫＰＳ公開部を受信する。そして、装置WのＣＰＵ１０３１は、ステップＳ１０５７において、受信した暗号側のＫＰＳ公開部を記憶する。

[0132] また、装置ＵのＣＰＵ１０１１は、ステップＳ１０１９において、受領したＫＰＳ公開部を装置WのＣＰＵ１０３１に対して伝送し、装置WのＣＰＵ１０３１から伝送された装置WのＫＰＳ公開部を受信する。そして、装置ＵのＣＰＵ１０１１は、ステップＳ１０２１において、受信した装置WのＫＰＳ公開部を記憶する。

[0133] 一方、装置WのＣＰＵ１０３１は、ステップＳ１０５９において、受領したＫＰＳ公開部を装置ＵのＣＰＵ１０１１に対して伝送し、装置ＵのＣＰＵ１０１１から伝送された装置ＵのＫＰＳ公開部を受信する。そして、装置WのＣＰＵ１０３１は、ステップＳ１０６１において、受信した装置ＵのＫＰＳ公開部を記憶する。

[0134] 《通信装置》

図１１Ａ～図１１Ｄを参照して、本実施形態の通信装置Ｕ／Ｖ／Ｗの構成および動作について説明する。

[0135] （公開情報テーブル）

図１１Ａは、本実施形態に係る通信装置Ｕ／Ｖ／Ｗに記憶される公開情報

テーブル１１１０／１１２０／１１３０の構成を示す図である。ここで、公開情報テーブル１１１０は装置Ｕが保持する。公開情報テーブル１１２０は装置Ｖが保持する。公開情報テーブル１１３０は装置Wが保持する。なお、図１１Ａにおける具体値は、図６Ｄに示したBlomアルゴリズムの具体例に対応している。

[0136] 公開情報テーブル１１１０は、送信相手の装置ＩＤ１１１１に対応付けて、送信相手から伝送された送信相手の公開情報（公開部）１１１２を記憶する。すなわち、公開情報テーブル１１１０においては、装置Ｖと装置Wとから公開情報（公開部）１１１２を伝送され、送信相手と対応付けて記憶している。装置Ｕにおいて、平文を暗号化して暗号文を送信する、あるいは、受信した暗号文を復号して平文を生成する場合に、その通信相手が装置Ｖの場合には公開部としてγv=7が使用され、その通信相手が装置Wの場合には公開部としてγw=1が使用されることにより、ＴＰＭに保持された同じ秘密部を使用して通信相手と同じ共通鍵が生成される。

[0137] 公開情報テーブル１１２０は、送信相手の装置ＩＤ１１２１に対応付けて、送信相手から伝送された送信相手の公開情報（公開部）１１２２を記憶する。すなわち、公開情報テーブル１１２０においては、装置Ｕと装置Wとから公開情報（公開部）１１２２を伝送され、送信相手と対応付けて記憶している。また、公開情報テーブル１１３０は、送信相手の装置ＩＤ１１３１に対応付けて、送信相手から伝送された送信相手の公開情報（公開部）１１３２を記憶する。すなわち、公開情報テーブル１１３０においては、装置Ｕと装置Ｖとから公開情報（公開部）１１３２を伝送され、送信相手と対応付けて記憶している。

[0138] なお、公開情報テーブル１１２０を使用した装置Ｖの処理、および、公開情報テーブル１１３０を使用した装置Wの処理は、公開情報テーブル１１１０を使用した装置Ｕの処理と同様であるので、説明を省略する。

[0139] （運用準備処理手順）

図１１Ｂは、本実施形態に係る通信装置Ｕ／Ｖ／Wの運用準備処理の手順

を示すフローチャートである。なお、図１１Ｂにおいて、図４Ｂと同様のステップには同じステップ番号を付して、重複する説明を省略する。

[0140] 通信装置Ｕ／Ｖ／Ｗは、ステップＳ１１１９において、通信相手の装置ＩＤと、受信した通信相手のＫＰＳ公開部とを対応付けて、公開情報テーブルに記憶する。

[0141] （暗号文送信処理手順）

図１１Ｃは、本実施形態に係る通信装置Ｕ／Ｖ／Ｗの暗号文送信処理の手順を示すフローチャートである。なお、図１１Ｃにおいて、図４Ｃと同様のステップには同じステップ番号を付して、重複する説明を省略する。

[0142] 通信装置Ｕ／Ｖ／Ｗは、ステップＳ１１２３において、暗号文の送信先に対応付いた公開情報を公開情報テーブルから読み出す。

[0143] （平文復号処理手順）

図１１Ｄは、本実施形態に係る通信装置Ｕ／Ｖ／Ｗの平文復号処理の手順を示すフローチャートである。なお、図１１Ｄにおいて、図４Ｄと同様のステップには同じステップ番号を付して、重複する説明を省略する。

[0144] 通信装置Ｕ／Ｖ／Ｗは、ステップＳ１１３３において、暗号文の送信元に対応付いた公開情報を公開情報テーブルから読み出す。

[0145] 本実施形態によれば、３台以上の通信装置間でお互いに共通鍵方式で暗号通信する場合に、各通信装置において暗号化や復号時にＴＰＭ内で共通鍵を生成して、ＴＰＭ内で暗号化や復号を行ない、終了後には共通鍵を破棄することにより、共通鍵の漏洩を防いで、通信情報の秘匿性を高めることができる。

[0146] ［第５実施形態］

次に、本発明の第５実施形態に係る暗号通信システムについて説明する。本実施形態に係る暗号通信システムは、上記第２実施形態から第４実施形態と比べると、ＴＰＭがアプリケーションに対応する記憶を有しない点で異なる。本実施形態においては、サーバあるいは記憶媒体からダウンロードされたアプリケーションにより、ＴＰＭが上記実施形態の機能を獲得する。その

他の構成および動作は、第２実施形態から第４実施形態と同様であるため、同じ構成および動作については同じ符号を付してその詳しい説明を省略する。

[0147] （アプリケーションのダウンロード処理シーケンス）

図１２は、本実施形態に係る暗号通信システム１２００のアプリケーションのダウンロード処理の動作手順を示すシーケンス図である。図１２において、通信装置１２１０は本実施形態に従った暗号通信機能を有しないとする。特に、ＴＰＭ１２１２が本実施形態に従った暗号通信機能を有しない場合に対応する。なお、図１２において、図２Ａと同様のステップには同じステップ番号を付して、重複する説明を省略する。

[0148] 通信装置１２１０のＣＰＵ１２１１は、ステップＳ１２０１において、本実施形態に従った暗号通信のアプリケーションを提供するサーバあるいは記憶媒体１２２０に対してログインし、本実施形態に従った暗号通信のアプリケーションをダウンロードする。

[0149] 通信装置１２１０のＣＰＵ１２１１は、ステップＳ１２０３において、ＴＰＭ１２１２に用意されてない新たなコマンドフォーマットの埋込指示を行なう。ＴＰＭ１２１２は、ステップＳ１２０５において、新たなコマンドフォーマットを不揮発メモリに記憶する。

[0150] 通信装置１２１０のＣＰＵ１２１１は、ステップＳ１２０７において、ＴＰＭ１２１２に用意されてない新たな処理プログラムの埋込指示を行なう。ＴＰＭ１２１２は、ステップＳ１２０９において、新たな処理プログラムをプログラム領域に記憶する。

[0151] 以降は、ＴＰＭ１２１２が、本実施形態のEncryptコマンドやDecryptコマンドに対応して、処理プログラムに従った、秘密部の保持、共通鍵生成、暗号化および復号、を実現できるようになる。

[0152] 本実施形態によれば、あらかじめ通信装置またはＴＰＭが本実施形態の実現に必要な機能を有しなくとも、それら機能付与を通信装置またはＴＰＭにダウンロードすることにより、実現することができる。

[0153] ［他の実施形態］

なお、上記実施形態においては、通信装置が配布されたＫＰＳ秘密部をＴＭＰに埋め込む構成を示したが、あらかじめＴＭＰの製造時にＫＰＳ秘密部が埋め込まれており、対応するＫＳＰ公開部を取得して通信相手に伝送する構成であっても、本発明と同様の効果を奏することができる。

[0154] また、実施形態を参照して本発明を説明したが、本発明は上記実施形態に限定されるものではない。本発明の構成や詳細には、本発明のスコープ内で当業者が理解し得る様々な変更をすることができる。また、それぞれの実施形態に含まれる別々の特徴を如何様に組み合わせたシステムまたは装置も、本発明の範疇に含まれる。

[0155] また、本発明は、複数の機器から構成されるシステムに適用されてもよいし、単体の装置に適用されてもよい。さらに、本発明は、実施形態の機能を実現する情報処理プログラムが、システムあるいは装置に直接あるいは遠隔から供給される場合にも適用可能である。したがって、本発明の機能をコンピュータで実現するために、コンピュータにインストールされるプログラム、あるいはそのプログラムを保持した媒体、そのプログラムをダウンロードさせるWWW(World Wide Web)サーバも、本発明の範疇に含まれる。特に、少なくとも、上述した実施形態に含まれる処理ステップをコンピュータに実行させるプログラムを格納した非一時的コンピュータ可読媒体（non-transitory computer readable medium）は本発明の範疇に含まれる。

[0156] ［実施形態の他の表現］

上記の実施形態の一部または全部は、以下の付記のようにも記載されうるが、以下には限られない。

（付記１）

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信システムであって、

第１通信装置の第１セキュリティチップ（ＴＭＰ:Trusted Platform Modul

e)において、通信相手である第２通信装置から伝送された前記第２公開部を用いて前記第１セキュリティチップに保持された前記第１秘密部により共通鍵を生成し、前記第１セキュリティチップにおいて該共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成手段と、

前記第２通信装置の第２セキュリティチップにおいて、通信相手である前記第１通信装置から伝送された前記第１公開部を用いて前記第２セキュリティチップに保持された前記第２秘密部により共通鍵を生成し、前記第２セキュリティチップにおいて該共通鍵に基づいて、前記第１通信装置から受信した前記暗号文を復号して平文を生成する復号手段と、

を備える暗号通信システム。

（付記２）

前記暗号文生成手段および前記復号手段は、前記共通鍵に基づく暗号化または復号の後、前記共通鍵を破棄する、付記１に記載の暗号通信システム。

（付記３）

前記暗号鍵事前配布方式における秘密部と公開部との組のうち、前記秘密部をそれぞれの通信装置が有するセキュリティチップに保持すると共に、前記公開部を前記それぞれの通信装置の通信相手に伝送する運用準備手段をさらに備える付記１または２に記載の暗号通信システム。

（付記４）

前記暗号文生成手段と前記復号手段は、さらに、暗号化および復号をブロックごとに行なう場合の初期ベクタ（ＩＶ:Initialization Vector)を、前記セキュリティチップに保持された前記初期ベクタ用の秘密部と、前記通信相手から伝送された前記初期ベクタ用の公開部とから生成して、それぞれ前記暗号化および前記復号に使用する、付記１乃至３のいずれか１項に記載の暗号通信システム。

（付記５）

前記セキュリティチップに対して、

前記秘密部を受信して保持する秘密部保持手段と、

前記保持された秘密部と前記通信相手から伝送された公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

平文と前記通信相手から伝送された公開部とが添付された暗号化コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記平文を暗号化して暗号文を生成する暗号文生成手段と、

暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記暗号文を復号して平文を生成する復号手段と、

の少なくとも１つを付与するためのプログラムおよびデータを記憶させる機能付与手段をさらに備える付記１乃至４のいずれか１項に記載の暗号通信システム。

（付記６）

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信方法であって、

第１通信装置の第１セキュリティチップ（ＴＭＰ:Trusted Platform Module)において、通信相手である第２通信装置から伝送された前記第２公開部を用いて前記第１セキュリティチップに保持された前記第１秘密部により共通鍵を生成し、前記第１セキュリティチップにおいて該共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成ステップと、

前記第２通信装置の第２セキュリティチップにおいて、通信相手である前記第１通信装置から伝送された前記第１公開部を用いて前記第２セキュリティチップに保持された前記第２秘密部により共通鍵を生成し、前記第２セキュリティチップにおいて該共通鍵に基づいて、前記第１通信装置から受信した前記暗号文を復号して平文を生成する復号ステップと、

を含む暗号通信方法。

（付記７）

前記暗号文生成ステップおよび前記復号ステップにおいて、前記共通鍵に基づく暗号化または復号の後、前記共通鍵が破棄される、付記６に記載の暗号通信方法。

（付記８）

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置であって、

前記セキュリティチップが、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成手段と、

該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成手段と、

を備える通信装置。

（付記９）

前記暗号文生成手段は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、付記８に記載の通信装置。

（付記１０）

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成ステップと、

を含む通信装置の制御方法。

（付記１１）

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御プログラムであって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成ステップと、

をコンピュータに実行させる通信装置の制御プログラム。

（付記１２）

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置であって、

前記セキュリティチップが、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成手段と、

該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号手段と、

を備える通信装置。

（付記１３）

前記復号手段は、前記共通鍵に基づく暗号化または復号の後、前記共通鍵を破棄する、付記１２に記載の通信装置。

（付記１４）

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号ステップと、

を含む通信装置の制御方法。

（付記１５）

セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号ステップと、

をコンピュータに実行させる通信装置の制御プログラム。

（付記１６）

通信装置が有するセキュリティチップ（ＴＭＰ:Trusted Platform Module)であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

前記保持された秘密部と通信相手から伝送された前記暗号鍵事前配布方式における公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

平文と前記通信相手から伝送された公開部とが添付された暗号化コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記平文を暗号化して暗号文を生成する暗号文生成手段と、

を備えるセキュリティチップ。

（付記１７）

前記暗号文生成手段は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、付記１６に記載のセキュリティチップ。

（付記１８）

暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記暗号文を復号して平文を生成する復号手段、

をさらに備える付記１６または１７に記載のセキュリティチップ。

（付記１９）

前記復号手段、は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、付記１８に記載のセキュリティチップ。

（付記２０）

通信装置が有するセキュリティチップ（ＴＭＰ:Trusted Platform Module）であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

前記保持された秘密部と通信相手から伝送された前記暗号鍵事前配布方式における公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づ

いて前記暗号文を復号して平文を生成する復号手段、

を備えるセキュリティチップ。

（付記２１）

前記復号手段、は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、付記２０に記載のセキュリティチップ。

[0157] この出願は、２０１６年３月１１日に出願された日本国特許出願　特願２０１６－０４８２４４号を基礎とする優先権を主張し、その開示の全てをここに取り込む。

請求の範囲

[請求項1] 暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信システムであって、

第１通信装置の第１セキュリティチップ（ＴＭＰ:Trusted Platform Module)において、通信相手である第２通信装置から伝送された前記第２公開部を用いて前記第１セキュリティチップに保持された前記第１秘密部により共通鍵を生成し、前記第１セキュリティチップにおいて該共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成手段と、

前記第２通信装置の第２セキュリティチップにおいて、通信相手である前記第１通信装置から伝送された前記第１公開部を用いて前記第２セキュリティチップに保持された前記第２秘密部により共通鍵を生成し、前記第２セキュリティチップにおいて該共通鍵に基づいて、前記第１通信装置から受信した前記暗号文を復号して平文を生成する復号手段と、

を備える暗号通信システム。

[請求項2] 前記暗号文生成手段および前記復号手段は、前記共通鍵に基づく暗号化または復号の後、前記共通鍵を破棄する、請求項１に記載の暗号通信システム。

[請求項3] 前記暗号鍵事前配布方式における秘密部と公開部との組のうち、前記秘密部をそれぞれの通信装置が有するセキュリティチップに保持すると共に、前記公開部を前記それぞれの通信装置の通信相手に伝送する運用準備手段をさらに備える請求項１または２に記載の暗号通信システム。

[請求項4] 前記暗号文生成手段と前記復号手段は、さらに、暗号化および復号をブロックごとに行なう場合の初期ベクタ（ＩＶ:Initialization Vector)を、前記セキュリティチップに保持された前記初期ベクタ用の

秘密部と、前記通信相手から伝送された前記初期ベクタ用の公開部とから生成して、それぞれ前記暗号化および前記復号に使用する、請求項１乃至３のいずれか１項に記載の暗号通信システム。

[請求項5] 前記セキュリティチップに対して、

前記秘密部を受信して保持する秘密部保持手段と、

前記保持された秘密部と前記通信相手から伝送された公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

平文と前記通信相手から伝送された公開部とが添付された暗号化コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記平文を暗号化して暗号文を生成する暗号文生成手段と、

暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記暗号文を復号して平文を生成する復号手段と、

の少なくとも１つを付与するためのプログラムおよびデータを記憶させる機能付与手段をさらに備える請求項１乃至４のいずれか１項に記載の暗号通信システム。

[請求項6] 暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における第１秘密部と第１公開部との組、および、第２秘密部と第２公開部との組を用いる暗号通信方法であって、

第１通信装置の第１セキュリティチップ（ＴＭＰ:Trusted Platform Module)において、通信相手である第２通信装置から伝送された前記第２公開部を用いて前記第１セキュリティチップに保持された前記第１秘密部により共通鍵を生成し、前記第１セキュリティチップにおいて該共通鍵に基づいて平文を暗号化して暗号文を生成する暗号文生成ステップと、

前記第２通信装置の第２セキュリティチップにおいて、通信相手である前記第１通信装置から伝送された前記第１公開部を用いて前記第２セキュリティチップに保持された前記第２秘密部により共通鍵を生成し、前記第２セキュリティチップにおいて該共通鍵に基づいて、前記第１通信装置から受信した前記暗号文を復号して平文を生成する復号ステップと、

を含む暗号通信方法。

[請求項7] 前記暗号文生成ステップおよび前記復号ステップにおいて、前記共通鍵に基づく暗号化または復号の後、前記共通鍵が破棄される、請求項６に記載の暗号通信方法。

[請求項8] セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置であって、

前記セキュリティチップが、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成手段と、

該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成手段と、

を備える通信装置。

[請求項9] 前記暗号文生成手段は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、請求項８に記載の通信装置。

[請求項10] セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成ステップと、

を含む通信装置の制御方法。

[請求項11] セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御プログラムであって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、平文を暗号化して暗号文を生成する暗号文生成ステップと、

をコンピュータに実行させる通信装置の制御プログラム。

[請求項12] セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置であって、

前記セキュリティチップが、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成手段と、

該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号手段と、

を備える通信装置。

[請求項13] 前記復号手段は、前記共通鍵に基づく暗号化または復号の後、前記共通鍵を破棄する、請求項１２に記載の通信装置。

[請求項14] セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号ステップと、

を含む通信装置の制御方法。

[請求項15] セキュリティチップ（ＴＭＰ:Trusted Platform Module)を有する通信装置の制御方法であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を、前記セキュリティチップの秘密部保持手段に保持する秘密部保持ステップと、

前記セキュリティチップにおいて、通信相手から伝送された暗号鍵事前配布方式における公開部を用いて、前記保持された秘密部により共通鍵を生成する共通鍵生成ステップと、

前記セキュリティチップにおいて、該共通鍵に基づいて、前記通信相手から受信した暗号文を復号して平文を生成する復号ステップと、

をコンピュータに実行させる通信装置の制御プログラム。

[請求項16] 通信装置が有するセキュリティチップ（ＴＭＰ:Trusted Platform Module)であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

前記保持された秘密部と通信相手から伝送された前記暗号鍵事前配布方式における公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

平文と前記通信相手から伝送された公開部とが添付された暗号化コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記平文を暗号化して暗号文を生成する暗号文生成手段と、

を備えるセキュリティチップ。

[請求項17] 前記暗号文生成手段は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、請求項１６に記載のセキュリティチップ。

[請求項18] 暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記暗号文を復号して平文を生成する復号手段、

をさらに備える請求項１６または１７に記載のセキュリティチップ。

[請求項19] 前記復号手段、は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、請求項１８に記載のセキュリティチップ。

[請求項20] 通信装置が有するセキュリティチップ（ＴＭＰ:Trusted Platform Module)であって、

暗号鍵事前配布方式（ＫＰＳ:Key Predistribution System)における秘密部を保持する秘密部保持手段と、

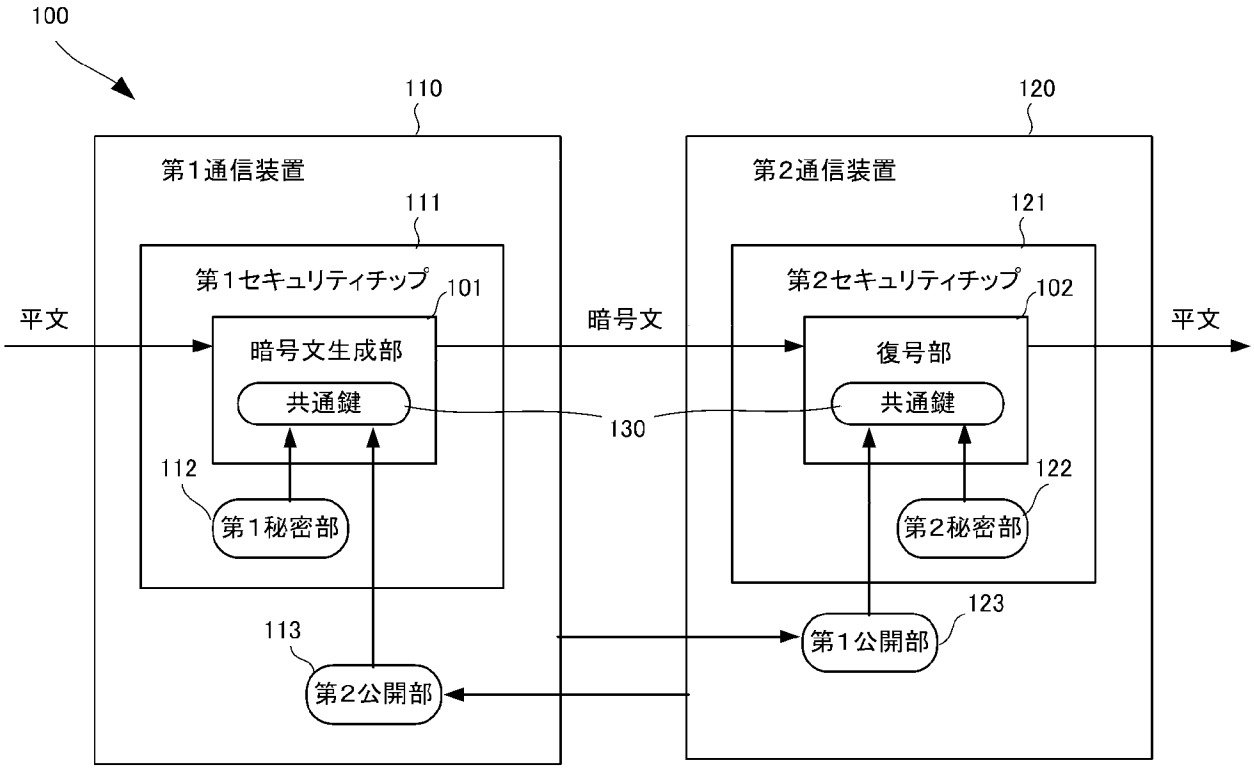
前記保持された秘密部と通信相手から伝送された前記暗号鍵事前配布方式における公開部とに基づいて、前記暗号鍵事前配布方式にしたがって共通鍵を生成する共通鍵生成手段と、

暗号文と前記通信相手から伝送された公開部とが添付された復号コマンドを受信して、前記共通鍵生成手段に前記共通鍵を生成させ、該共通鍵に基づいて前記暗号文を復号して平文を生成する復号手段、

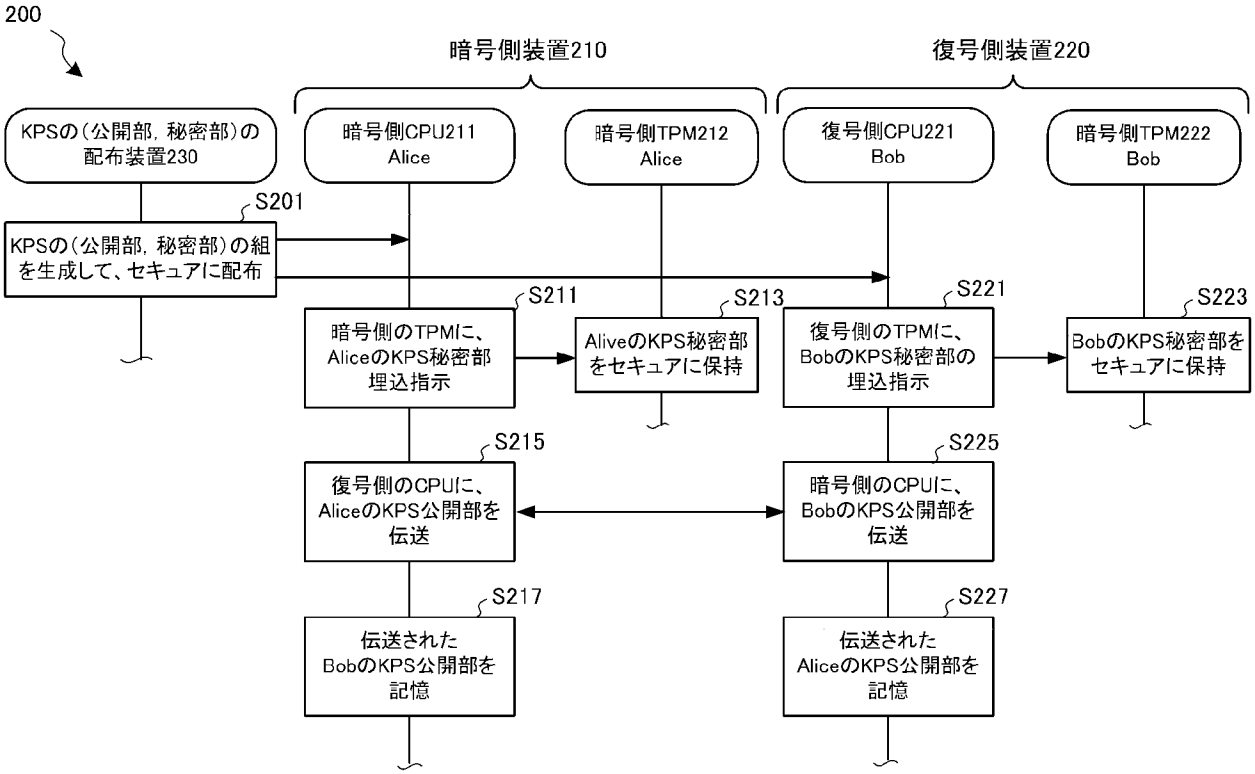
を備えるセキュリティチップ。

［請求項21］　前記復号手段、は、前記共通鍵に基づく暗号化の後、前記共通鍵を破棄する、請求項２０に記載のセキュリティチップ。

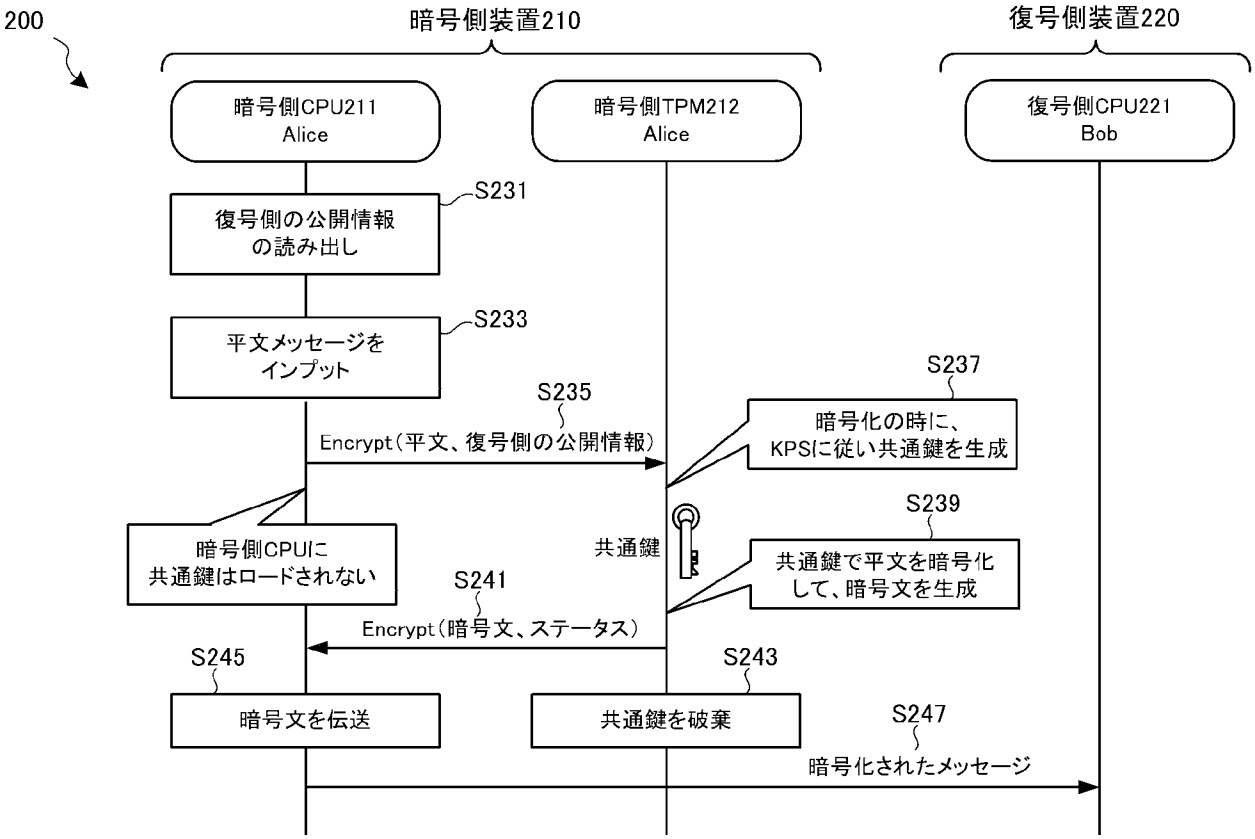
[図1]


100
110
第1通信装置
111
第1セキュリティチップ
101
平文
暗号文生成部
共通鍵
112
第1秘密部
113
第2公開部
130
120
第2通信装置
121
第2セキュリティチップ
102
暗号文
復号部
共通鍵
122
第2秘密部
123
第1公開部
平文

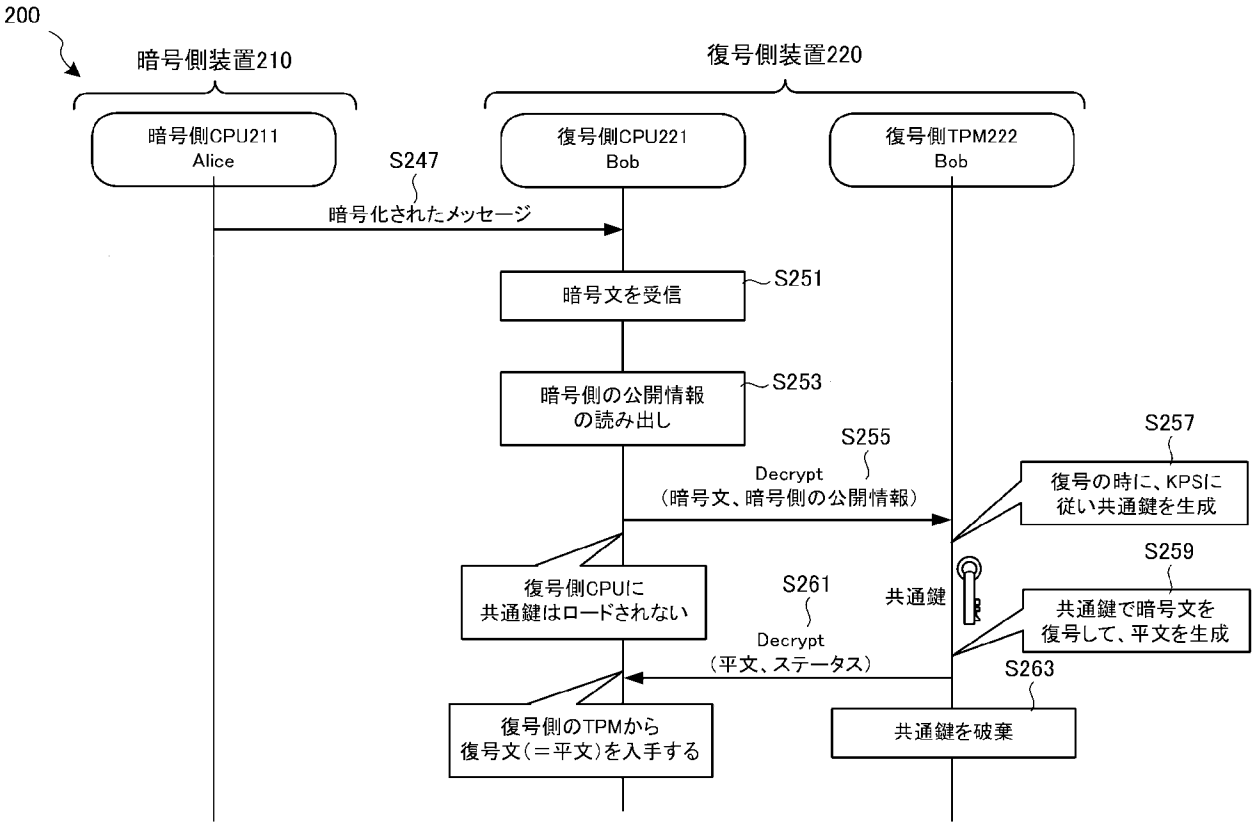
[図2A]


200
暗号側装置210
復号側装置220
KPSの(公開部, 秘密部)の配布装置230
暗号側CPU211 Alice
暗号側TPM212 Alice
復号側CPU221 Bob
暗号側TPM222 Bob
S201
KPSの(公開部, 秘密部)の組を生成して、セキュアに配布
S211
暗号側のTPMに、AliceのKPS秘密部埋込指示
S213
AliveのKPS秘密部をセキュアに保持
S221
復号側のTPMに、BobのKPS秘密部の埋込指示
S223
BobのKPS秘密部をセキュアに保持
S215
復号側のCPUに、AliceのKPS公開部を伝送
S225
暗号側のCPUに、BobのKPS公開部を伝送
S217
伝送されたBobのKPS公開部を記憶
S227
伝送されたAliceのKPS公開部を記憶

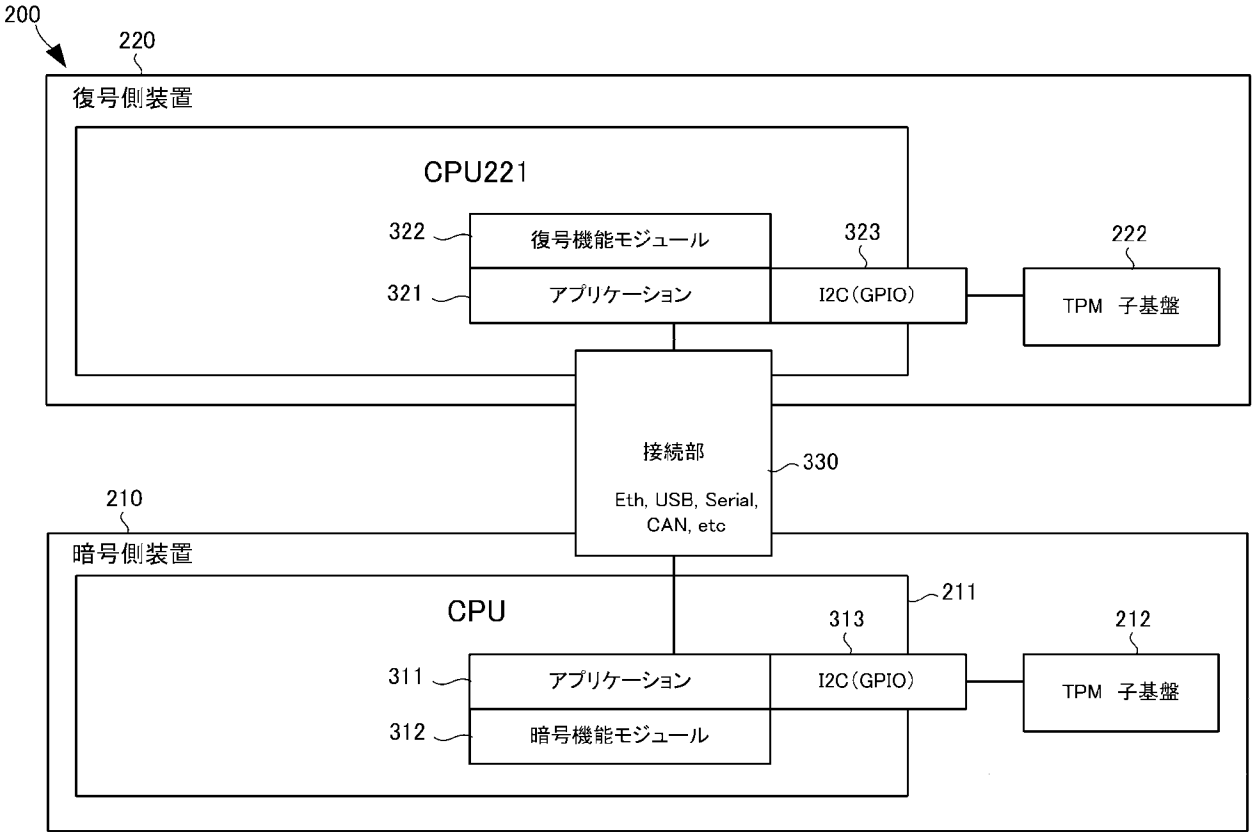
[図2B]


200
暗号側装置210
復号側装置220
暗号側CPU211
Alice
暗号側TPM212
Alice
復号側CPU221
Bob
S231
復号側の公開情報
の読み出し
S233
平文メッセージを
インプット
S235
Encrypt(平文、復号側の公開情報)
S237
暗号化の時に、
KPSに従い共通鍵を生成
S239
共通鍵で平文を暗号化
して、暗号文を生成
暗号側CPUに
共通鍵はロードされない
共通鍵
S241
Encrypt(暗号文、ステータス)
S245
暗号文を伝送
S243
共通鍵を破棄
S247
暗号化されたメッセージ

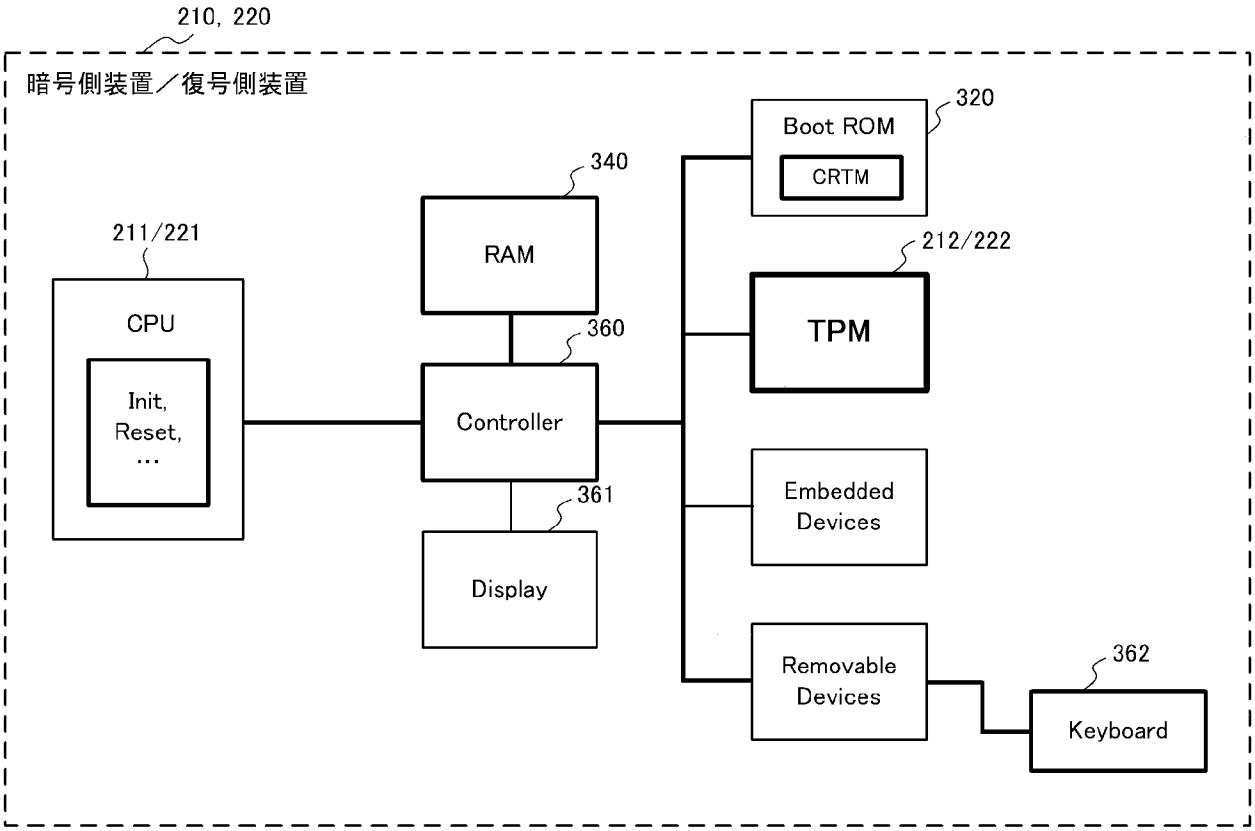
[図2C]


200
暗号側装置210
復号側装置220
暗号側CPU211
Alice
復号側CPU221
Bob
復号側TPM222
Bob
S247
暗号化されたメッセージ
暗号文を受信
S251
暗号側の公開情報
の読み出し
S253
S255
Decrypt
（暗号文、暗号側の公開情報）
S257
復号の時に、KPSに
従い共通鍵を生成
S259
共通鍵
共通鍵で暗号文を
復号して、平文を生成
復号側CPUに
共通鍵はロードされない
S261
Decrypt
（平文、ステータス）
S263
復号側のTPMから
復号文（＝平文）を入手する
共通鍵を破棄

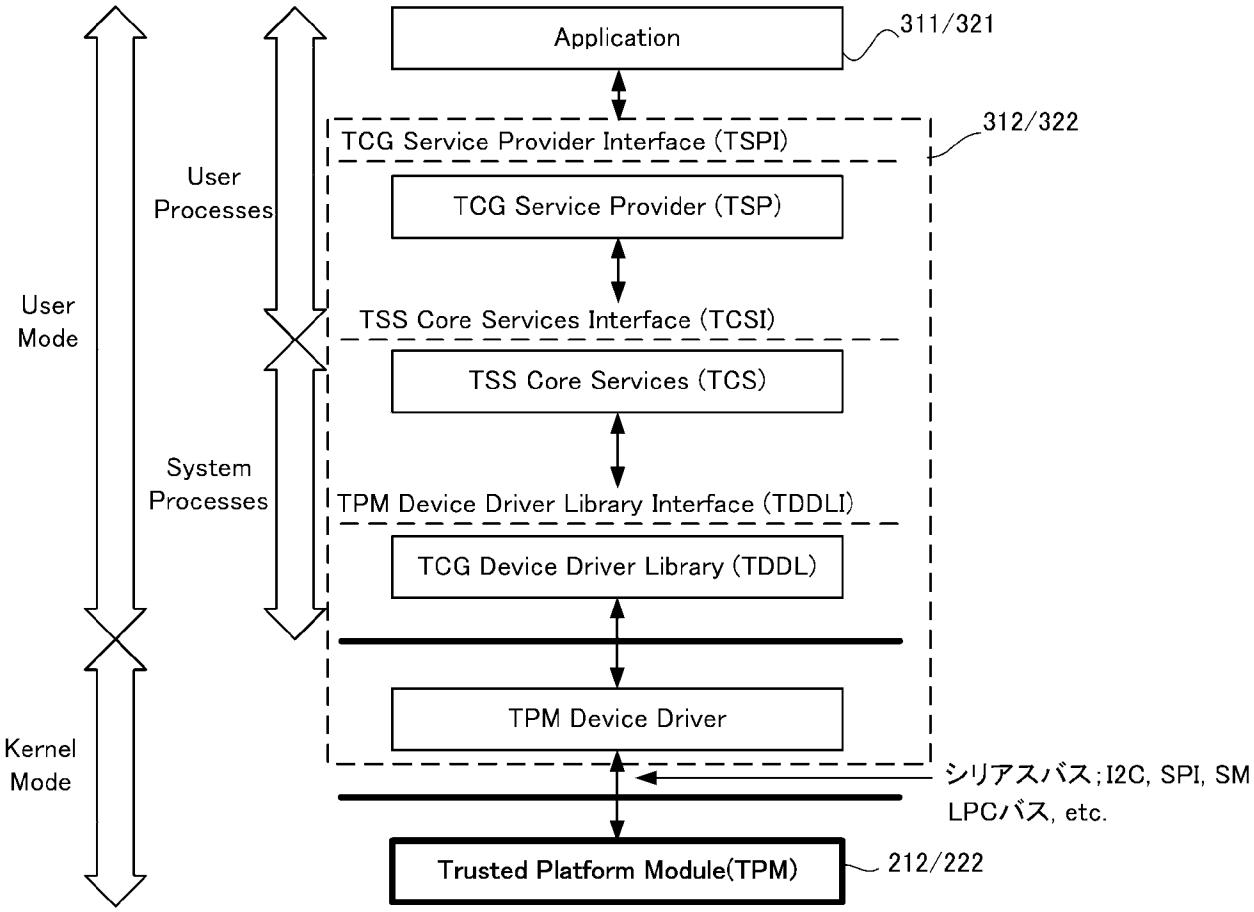
[図3A]


200
220
復号側装置
CPU221
322
復号機能モジュール
323
222
321
アプリケーション
I2C(GPIO)
TPM 子基盤
接続部
330
Eth, USB, Serial,
CAN, etc
210
暗号側装置
211
CPU
313
212
311
アプリケーション
I2C(GPIO)
TPM 子基盤
312
暗号機能モジュール

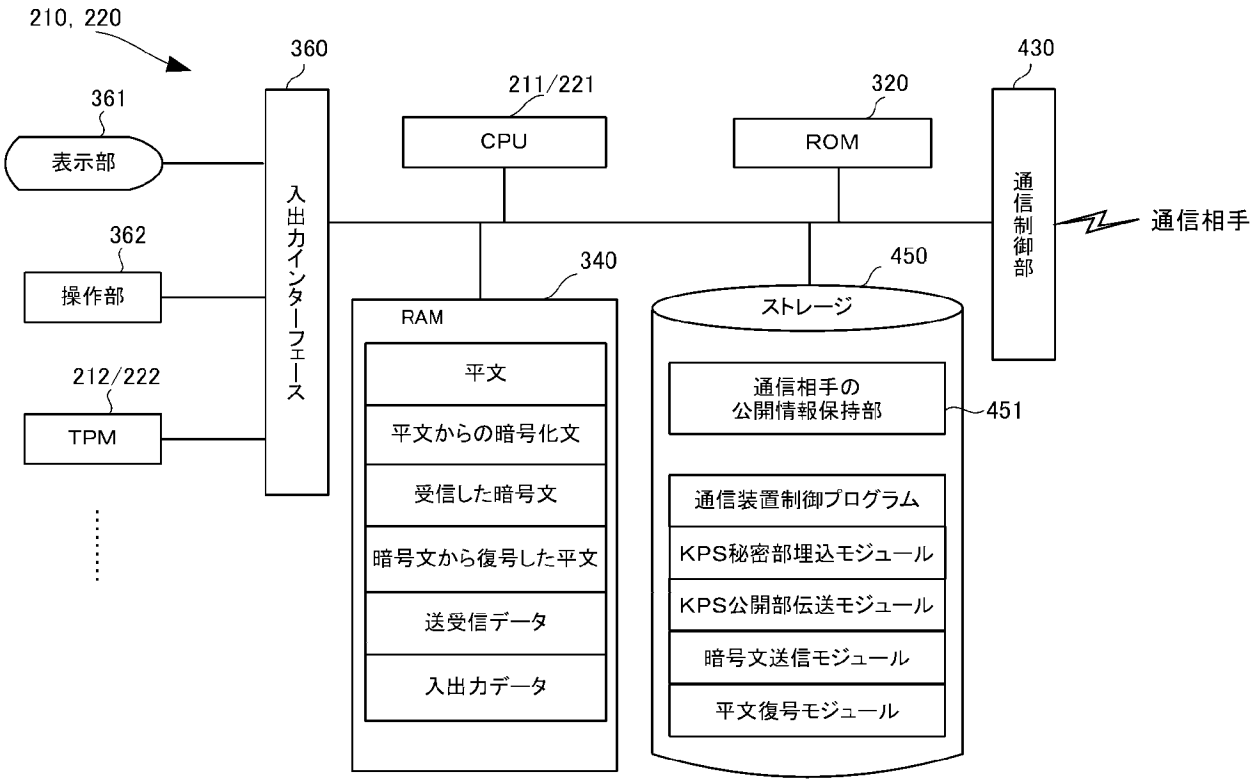
[図3B]


210, 220
暗号側装置／復号側装置
211/221
CPU
Init,
Reset,
…
RAM
340
Controller
360
Display
361
Boot ROM
CRTM
320
TPM
212/222
Embedded
Devices
Removable
Devices
362
Keyboard

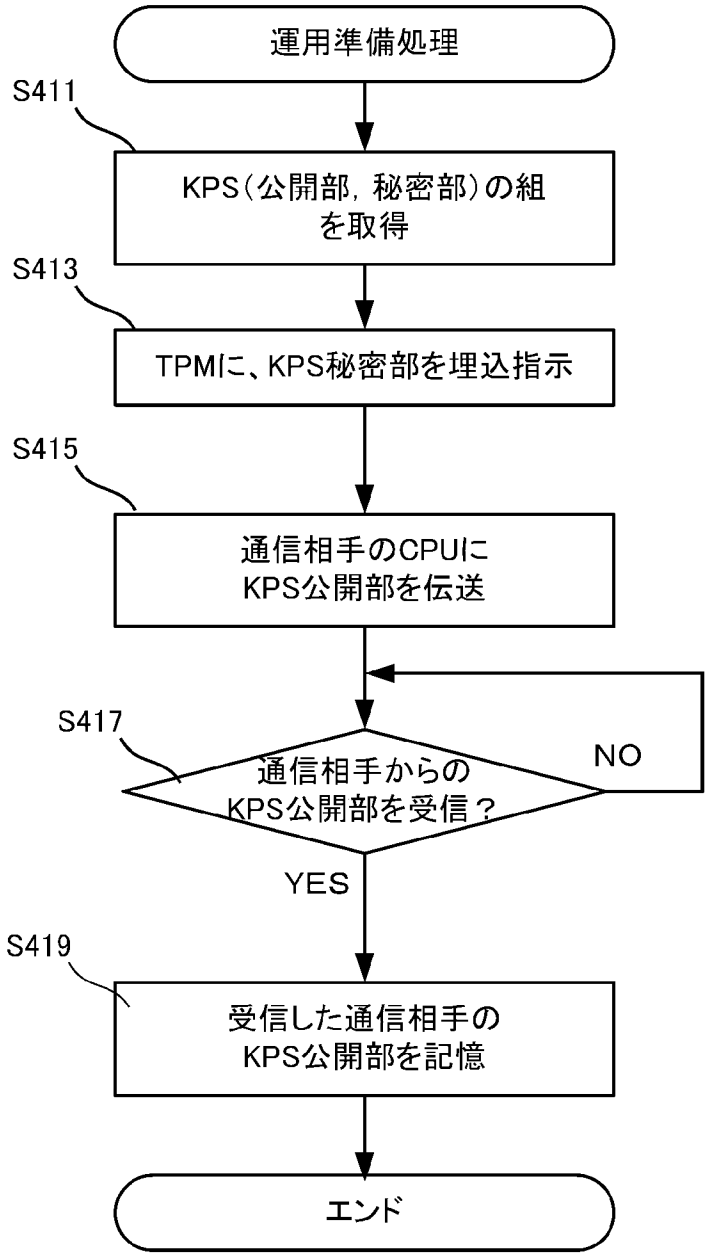
[図3C]


Application
311/321
TCG Service Provider Interface (TSPI)
312/322
TCG Service Provider (TSP)
TSS Core Services Interface (TCSI)
TSS Core Services (TCS)
TPM Device Driver Library Interface (TDDLI)
TCG Device Driver Library (TDDL)
TPM Device Driver
User Processes
System Processes
User Mode
Kernel Mode
シリアスバス;I2C, SPI, SM
LPCバス, etc.
Trusted Platform Module(TPM)
212/222

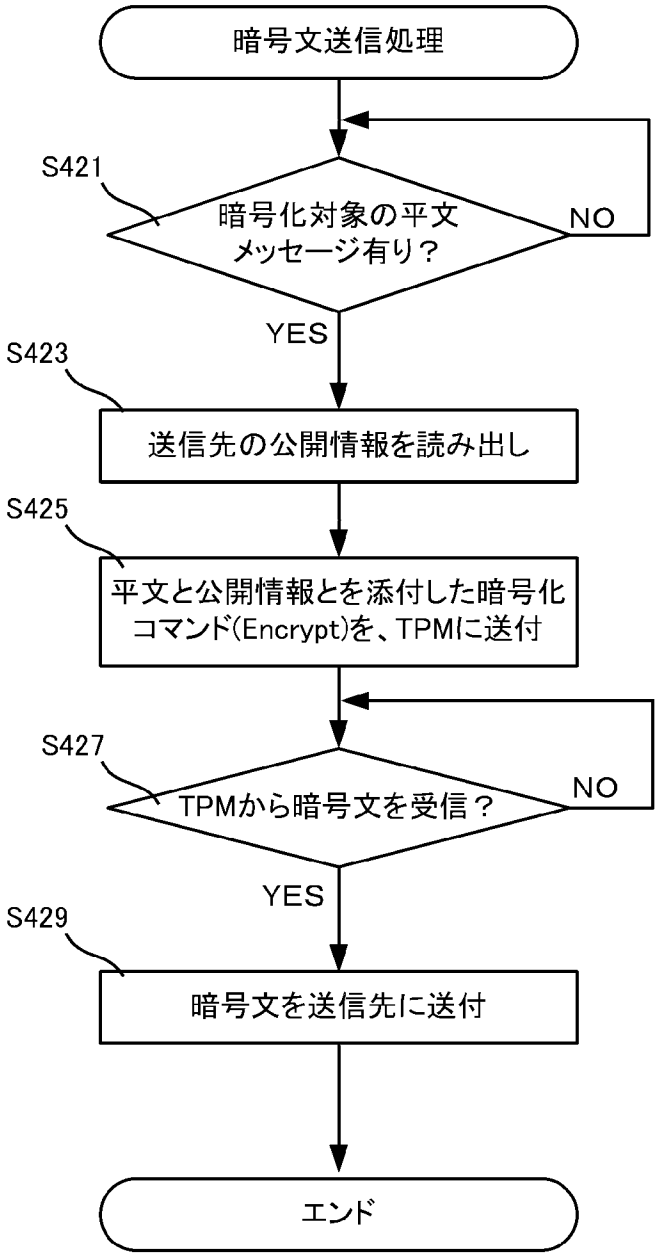
[図4A]


210, 220
360
361
表示部
入出力インターフェース
211/221
CPU
320
ROM
430
通信制御部
通信相手
362
操作部
340
RAM
平文
平文からの暗号化文
受信した暗号文
暗号文から復号した平文
送受信データ
入出力データ
450
ストレージ
通信相手の
公開情報保持部
451
212/222
TPM
通信装置制御プログラム
KPS秘密部埋込モジュール
KPS公開部伝送モジュール
暗号文送信モジュール
平文復号モジュール

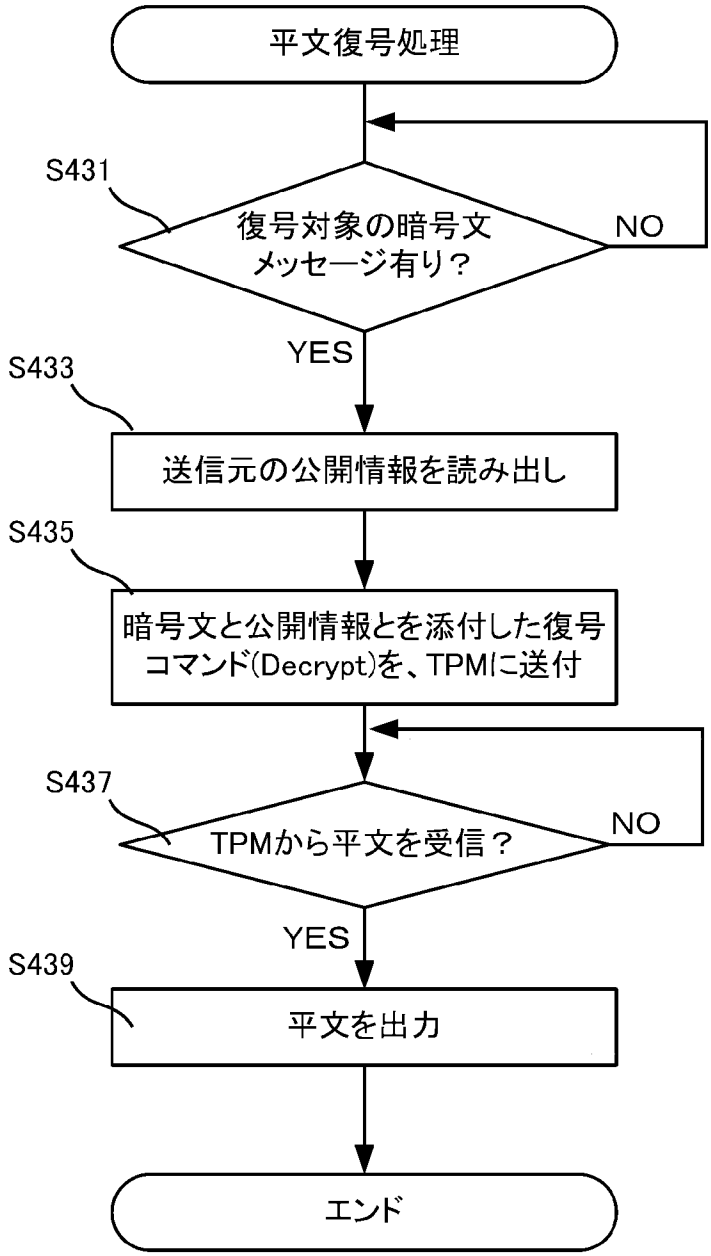
[図4B]


運用準備処理
S411
KPS(公開部，秘密部)の組を取得
S413
TPMに、KPS秘密部を埋込指示
S415
通信相手のCPUにKPS公開部を伝送
S417
通信相手からのKPS公開部を受信？
NO
YES
S419
受信した通信相手のKPS公開部を記憶
エンド

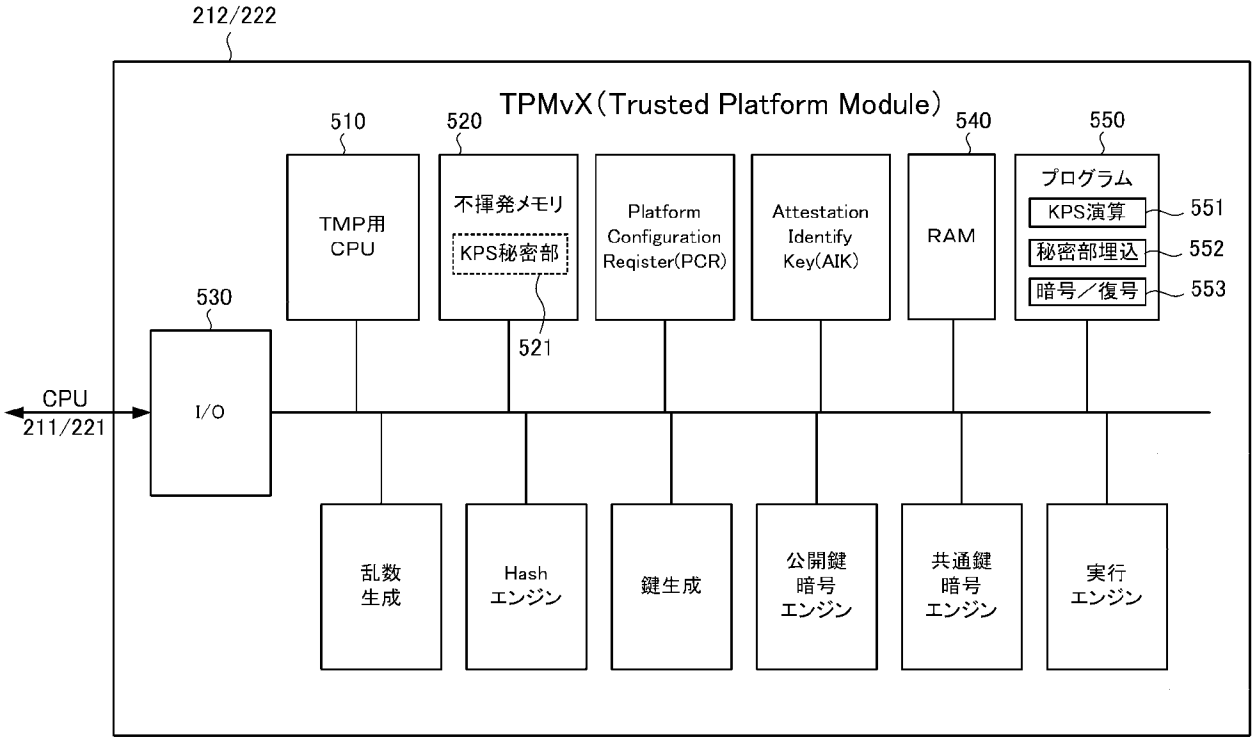
[図4C]


暗号文送信処理
S421
暗号化対象の平文
メッセージ有り？
NO
YES
S423
送信先の公開情報を読み出し
S425
平文と公開情報とを添付した暗号化
コマンド(Encrypt)を、TPMに送付
S427
TPMから暗号文を受信？
NO
YES
S429
暗号文を送信先に送付
エンド

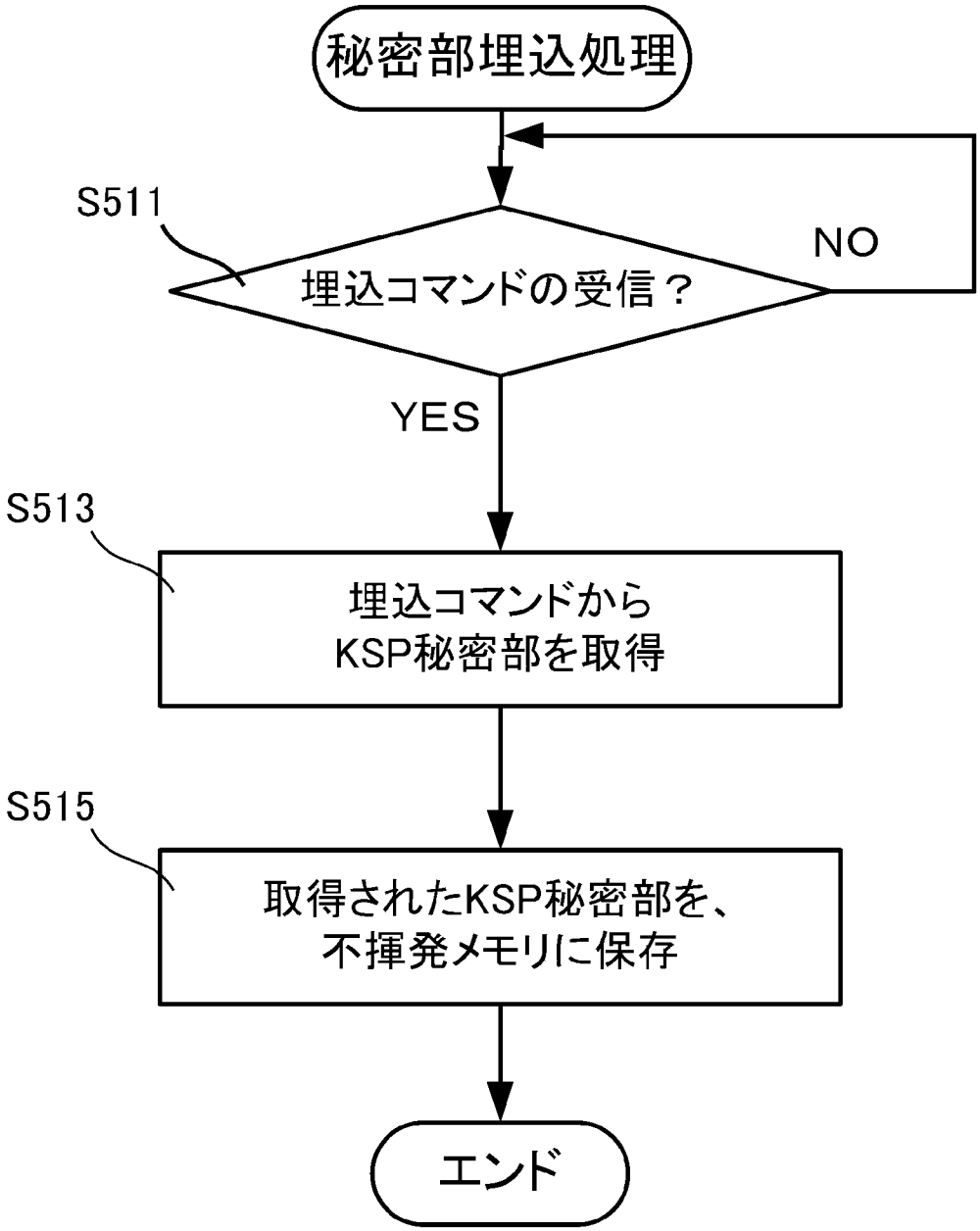
[図4D]


平文復号処理
S431
復号対象の暗号文
メッセージ有り？
NO
YES
S433
送信元の公開情報を読み出し
S435
暗号文と公開情報とを添付した復号
コマンド(Decrypt)を、TPMに送付
S437
TPMから平文を受信？
NO
YES
S439
平文を出力
エンド

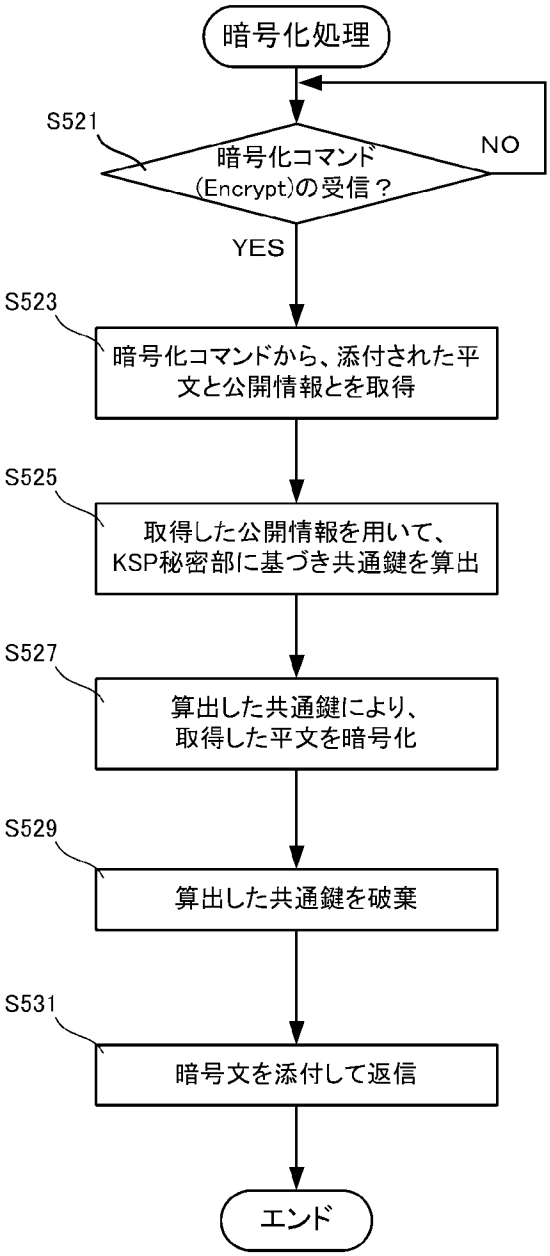
[図5A]


212/222
TPMvX(Trusted Platform Module)
510
520
540
550
TMP用
CPU
不揮発メモリ
KPS秘密部
Platform
Configuration
Reqister(PCR)
Attestation
Identify
Key(AIK)
RAM
プログラム
KPS演算
秘密部埋込
暗号／復号
551
552
553
530
521
CPU
211/221
I/O
乱数
生成
Hash
エンジン
鍵生成
公開鍵
暗号
エンジン
共通鍵
暗号
エンジン
実行
エンジン

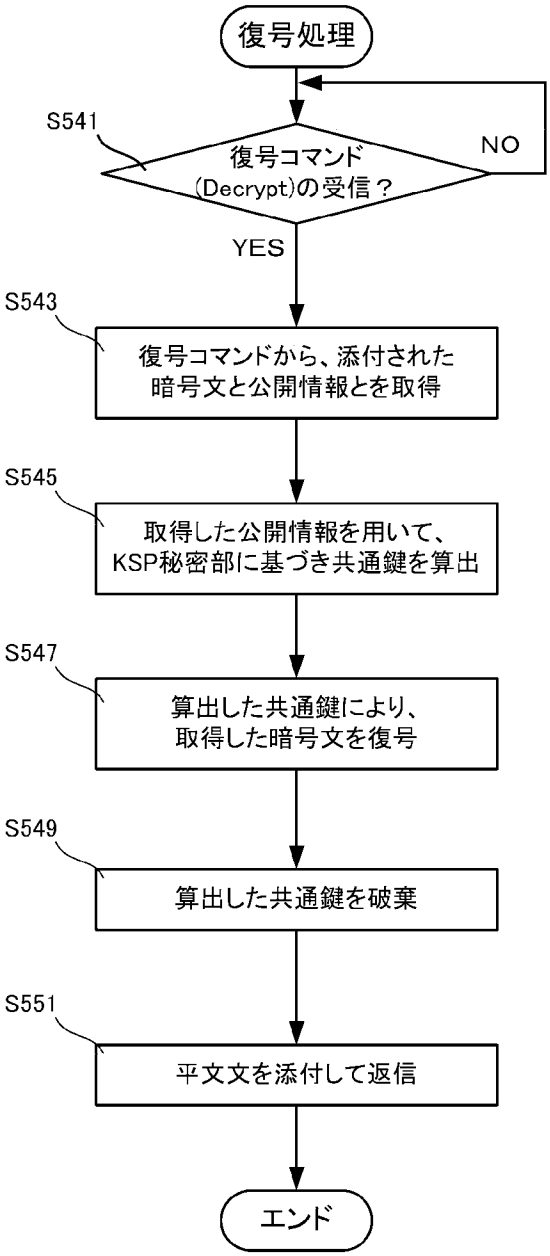
[図5B]


秘密部埋込処理
S511
埋込コマンドの受信？
NO
YES
S513
埋込コマンドから
KSP秘密部を取得
S515
取得されたKSP秘密部を、
不揮発メモリに保存
エンド

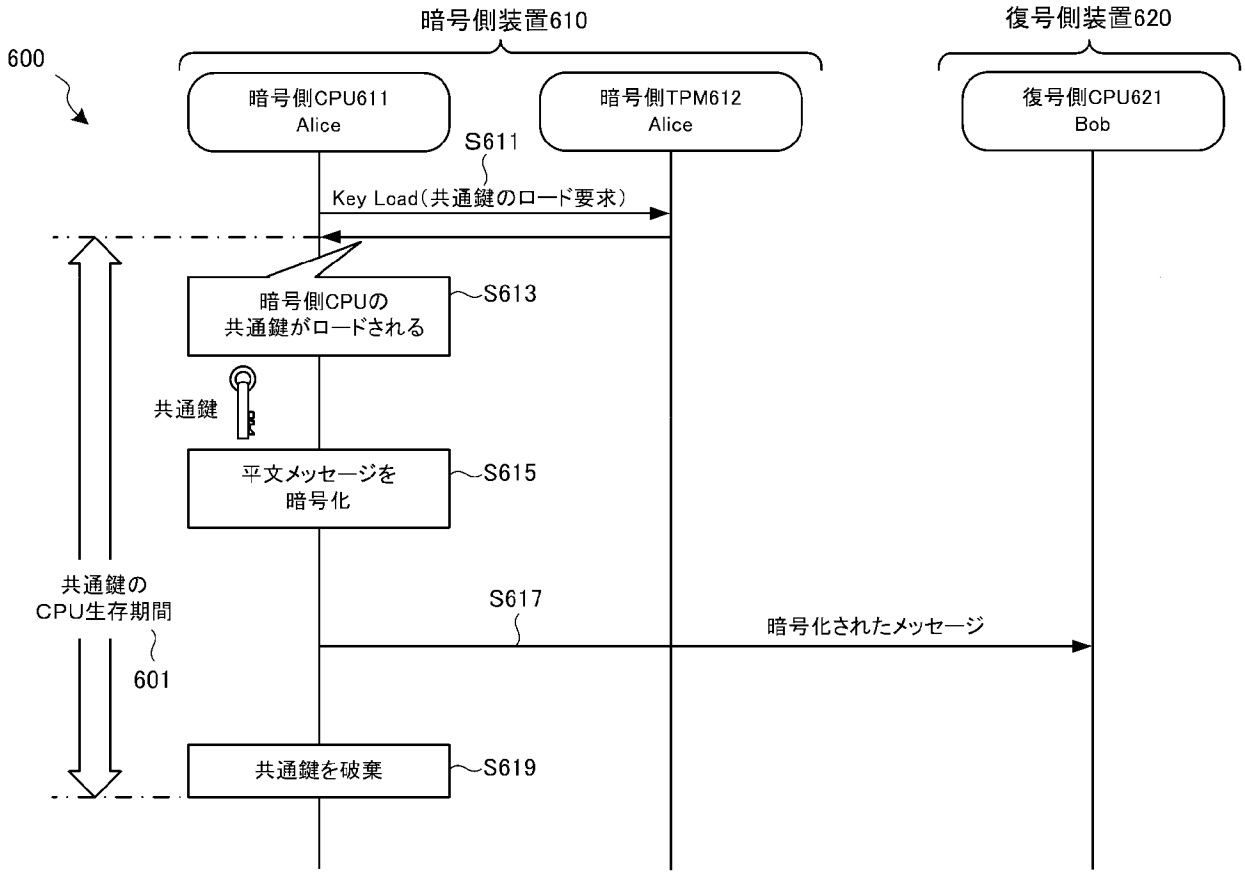
[図5C]


暗号化処理
S521
暗号化コマンド
(Encrypt)の受信？
NO
YES
S523
暗号化コマンドから、添付された平文と公開情報とを取得
S525
取得した公開情報を用いて、KSP秘密部に基づき共通鍵を算出
S527
算出した共通鍵により、取得した平文を暗号化
S529
算出した共通鍵を破棄
S531
暗号文を添付して返信
エンド

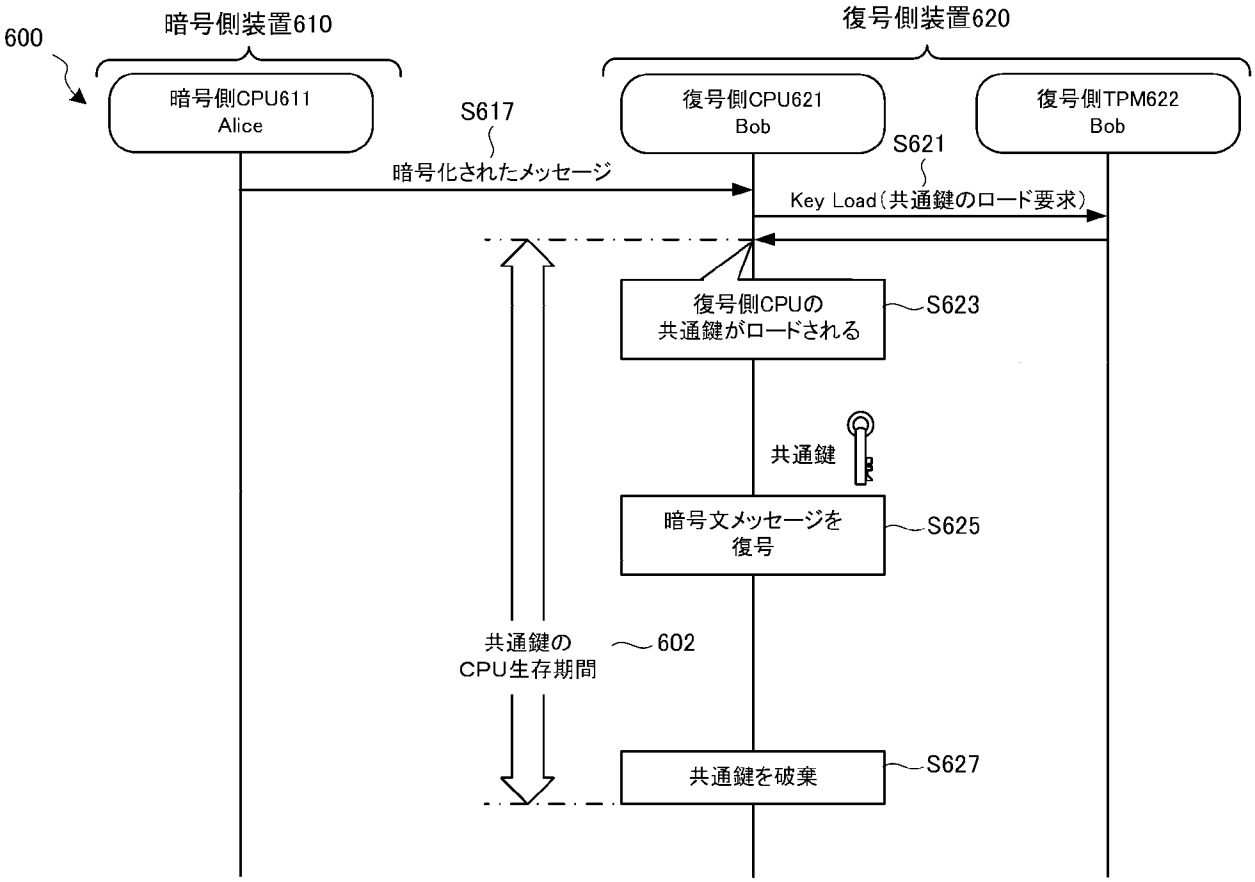
[図5D]


復号処理
S541
復号コマンド
(Decrypt)の受信？
NO
YES
S543
復号コマンドから、添付された
暗号文と公開情報とを取得
S545
取得した公開情報を用いて、
KSP秘密部に基づき共通鍵を算出
S547
算出した共通鍵により、
取得した暗号文を復号
S549
算出した共通鍵を破棄
S551
平文文を添付して返信
エンド

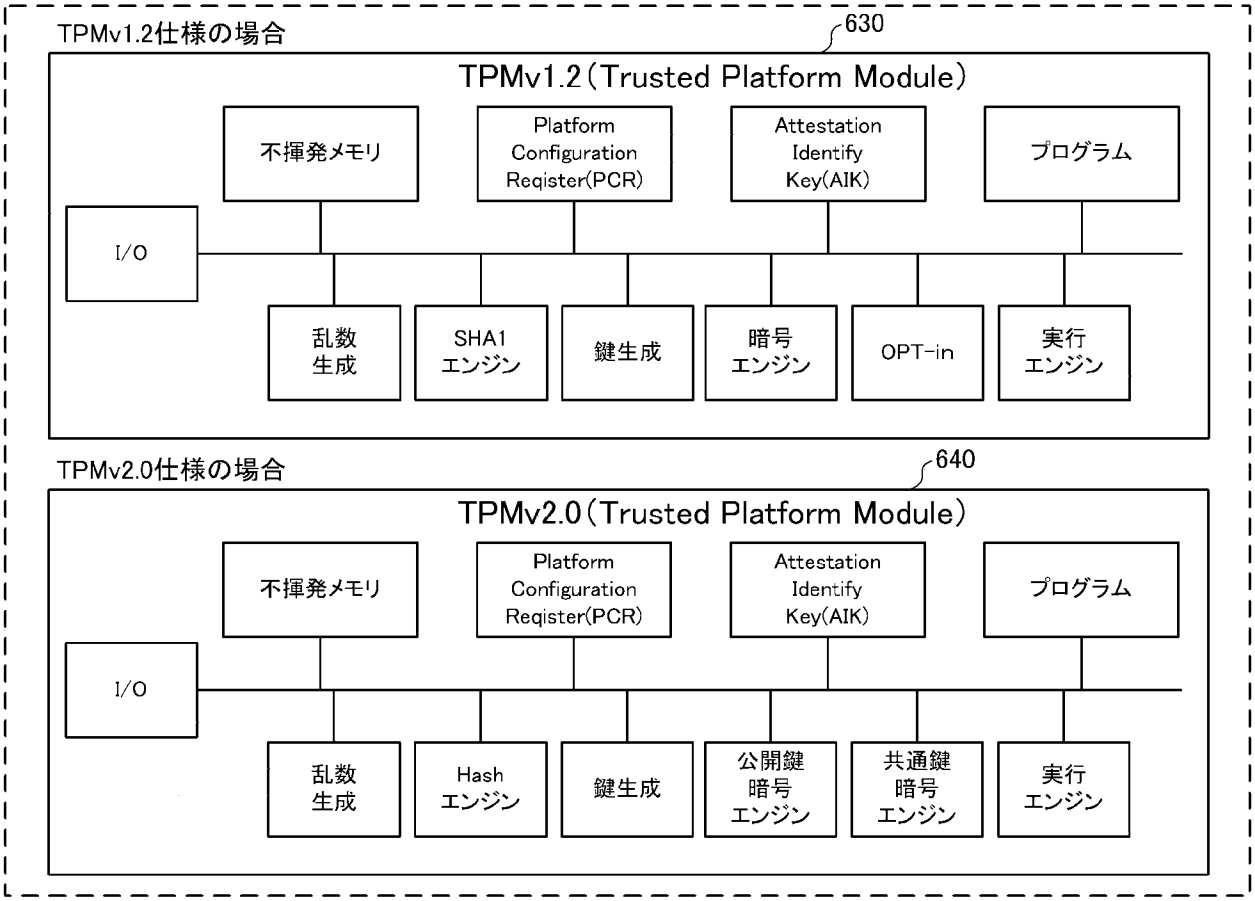
[図6A]


暗号側装置610
復号側装置620
600
暗号側CPU611
Alice
暗号側TPM612
Alice
復号側CPU621
Bob
S611
Key Load(共通鍵のロード要求)
暗号側CPUの
共通鍵がロードされる
S613
共通鍵
平文メッセージを
暗号化
S615
共通鍵の
CPU生存期間
601
S617
暗号化されたメッセージ
共通鍵を破棄
S619

[図6B]


600
暗号側装置610
暗号側CPU611
Alice
復号側装置620
復号側CPU621
Bob
復号側TPM622
Bob
S617
暗号化されたメッセージ
S621
Key Load（共通鍵のロード要求）
復号側CPUの
共通鍵がロードされる
S623
共通鍵
暗号文メッセージを
復号
S625
共通鍵の
CPU生存期間
602
共通鍵を破棄
S627

[図6C]


TPMv1.2仕様の場合
630
TPMv1.2(Trusted Platform Module)
不揮発メモリ
Platform Configuration Reqister(PCR)
Attestation Identify Key(AIK)
プログラム
I/O
乱数生成
SHA1エンジン
鍵生成
暗号エンジン
OPT-in
実行エンジン
TPMv2.0仕様の場合
640
TPMv2.0(Trusted Platform Module)
不揮発メモリ
Platform Configuration Reqister(PCR)
Attestation Identify Key(AIK)
プログラム
I/O
乱数生成
Hashエンジン
鍵生成
公開鍵暗号エンジン
共通鍵暗号エンジン
実行エンジン

[図6D]

650

KPS(Key Pre-Distribution Scheme)としてBlomアルゴリズム

<理論>

Here is Blom scheme for κ=1. For each node U, a value $\gamma u \in Z\_p$ is made public (where $p \geqq n$ is prime). The value γu are distinct elements of Z_p.

Protocol: Blom's key distribution scheme (κ=1)

The TA(Trusted Authority) chooses three random elements a, b, c $\in$ Z_p (not necessarily distinct), and forms the polynominal

f (x, y) = a + b (x + y) + cxy mod p.

For each node U, the TA computes the polynominal

gu (x) = f (x, γu) mod p = αu + βu x

and transmits (αu, βu) to U over a secure channel.

The Key for U and V is

Ku, v = Kv, u = f (γu, γv) = gu (γv) = gv (γu)

Where U computes Ku,v = gu (γu), and, V computes Kv, u = gv (γu).

We have αu = (a + bγu) mod p

βu = (b + cγu) mod p

gu (γu) = a + b (γu + γv) + cγuγv = f (γu, γv) mod p.

651

<具体例>

a=8, b=7, c=2, p=17, γu=12, γv=7, γw=1とすると、

f (x, y) = 8 + 7 (x + y) + 2xy

gu (x) = f (x, ru) mod p = (8 + 7 (x + 12) + 2*12x) mod 17 gv (x) = f (x, rv) mod p = (8 + 7 (x + 7) + 2*7x) mod 17

gw (x) = f (x, rw) mod p = (8 + 7 (x + 1) + 2*1x) mod 17

Ku, v = gu (v) = (8 + 7 (7 + 12) + 2*12*7) mod 17 = 3 Kv, u = gv (u) = (8 + 7 (12 + 7) + 2*7*12) mod 17 = 3

Ku, w = gu (w) = (8 + 7 (1 + 12) + 2*12*1) mod 17 = 4 Kw, u = gw (u) = (8 + 7 (12 + 1) + 2*1*12) mod 17 = 4

Kv, w = gv (w) = (8 + 7 (1 + 7) + 2*7*1) mod 17 = 10 Kw, v = gw (v) = (8 + 7 (7 + 1) + 2*1*7) mod 17 = 10

となり、Uの立場では、αu= (a + bγu) mod p = 7及びβu= (b + cγu) mod p = 14の値を、秘密に保持し(gu (x) = (7 + 14x) mod 17)、

Vの立場では、αv= (a + bγv) mod p = 6及びβv= (b + cγv) mod p = 4の値を、秘密に保持し(gu (x) = (6 + 4x) mod 17)、

Wの立場では、αw= (a + bγw) mod p = 15及びβw= (b + cγw) mod p = 9の値を、秘密に保持する(gu (x) = (15 + 9x) mod 17)。

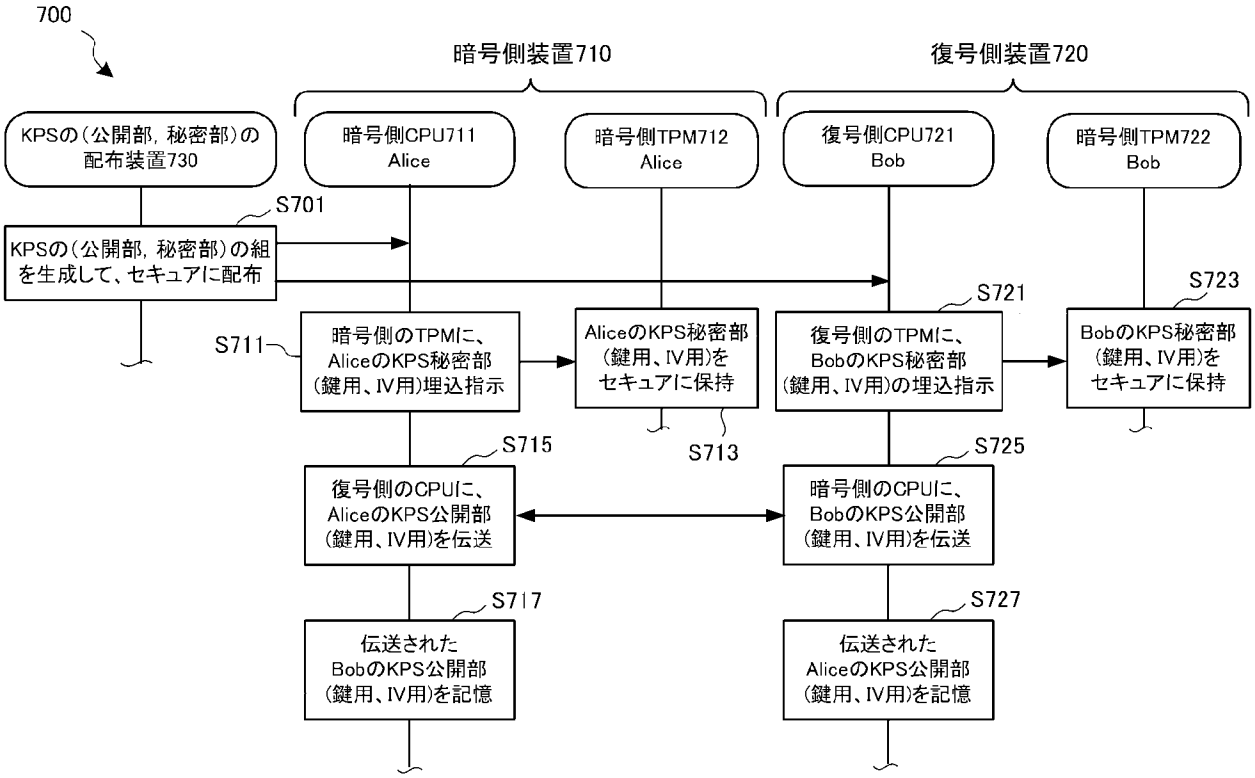
652

UはVが公開したγv=7の値を受信し、VはUが公開したγu=12の値を受信することで、UとVの共有値 Ku, v = Kv, u = gu (γv) = gv (γu) = 3が得られ、U,Vで共有する共通鍵として使用する。

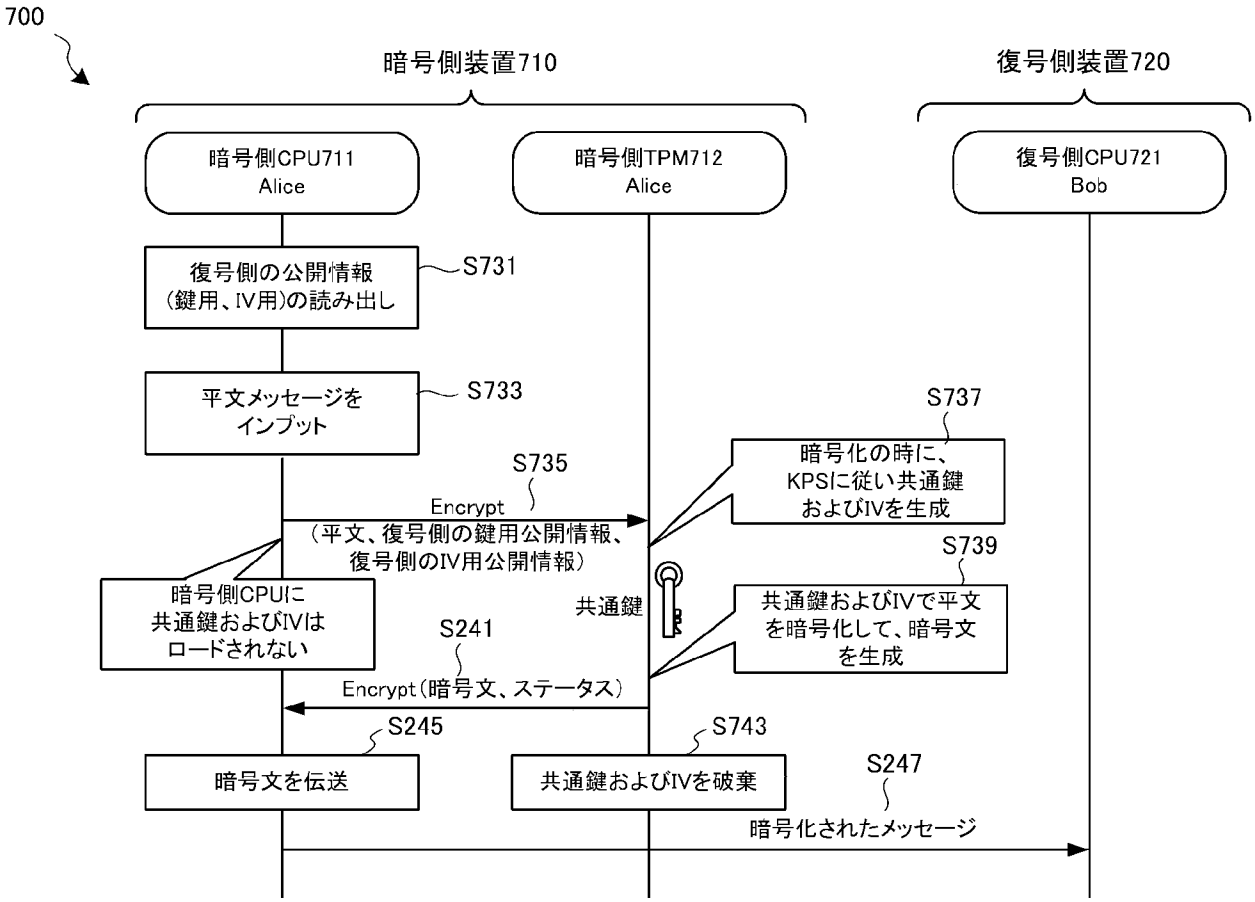
UはWが公開したγw=1の値を受信し、WはUが公開したγu=12の値を受信することで、UとWの共有値 Ku, w = Kw, u = gu (γw) = gw (γu) = 4が得られ、U,Wで共有する共通鍵として使用する。

WはVが公開したγv=7の値を受信し、VはWが公開したγu=1の値を受信することで、VとWの共有値 Kw, v = Kv, w = gw (γv) = gv (γw) = 10が得られ、W,Vで共有する共通鍵として使用する。

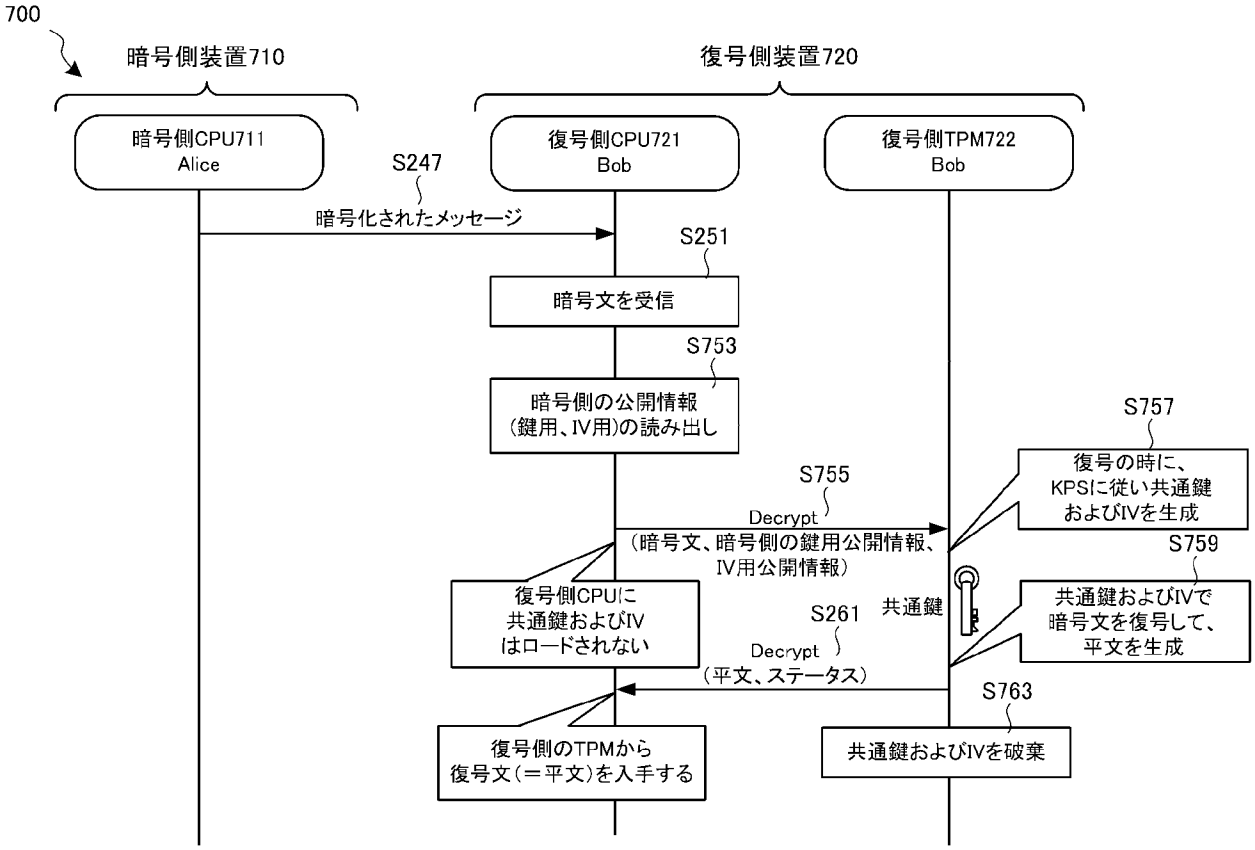
[図7A]


700
暗号側装置710
復号側装置720
KPSの(公開部, 秘密部)の配布装置730
暗号側CPU711 Alice
暗号側TPM712 Alice
復号側CPU721 Bob
暗号側TPM722 Bob
S701
KPSの(公開部, 秘密部)の組を生成して、セキュアに配布
S711
暗号側のTPMに、AliceのKPS秘密部(鍵用、IV用)埋込指示
AliceのKPS秘密部(鍵用、IV用)をセキュアに保持
S713
S721
復号側のTPMに、BobのKPS秘密部(鍵用、IV用)の埋込指示
S723
BobのKPS秘密部(鍵用、IV用)をセキュアに保持
S715
復号側のCPUに、AliceのKPS公開部(鍵用、IV用)を伝送
S725
暗号側のCPUに、BobのKPS公開部(鍵用、IV用)を伝送
S717
伝送されたBobのKPS公開部(鍵用、IV用)を記憶
S727
伝送されたAliceのKPS公開部(鍵用、IV用)を記憶

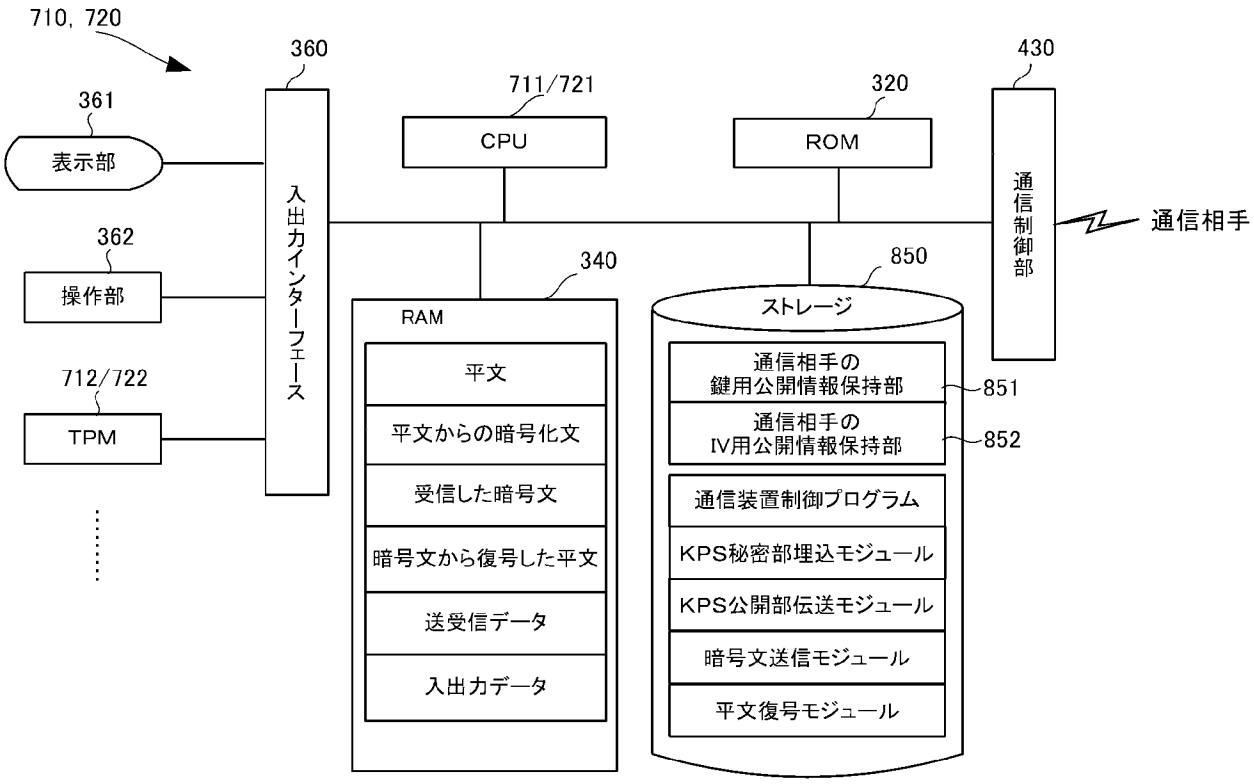
[図7B]


700
暗号側装置710
復号側装置720
暗号側CPU711
Alice
暗号側TPM712
Alice
復号側CPU721
Bob
復号側の公開情報
(鍵用、IV用)の読み出し
S731
平文メッセージを
インプット
S733
S737
暗号化の時に、
KPSに従い共通鍵
およびIVを生成
S735
Encrypt
(平文、復号側の鍵用公開情報、
復号側のIV用公開情報)
S739
暗号側CPUに
共通鍵およびIVは
ロードされない
共通鍵
共通鍵およびIVで平文
を暗号化して、暗号文
を生成
S241
Encrypt(暗号文、ステータス)
S245
S743
暗号文を伝送
共通鍵およびIVを破棄
S247
暗号化されたメッセージ

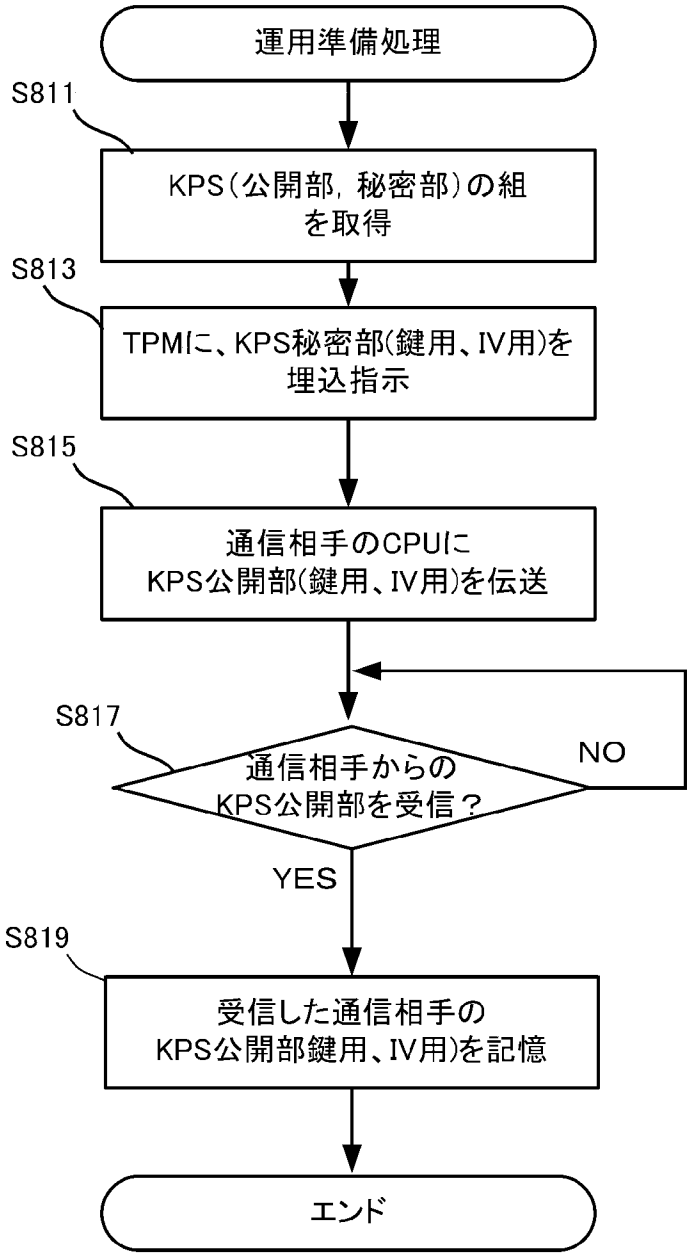
[図7C]


700
暗号側装置710
復号側装置720
暗号側CPU711
Alice
復号側CPU721
Bob
復号側TPM722
Bob
S247
暗号化されたメッセージ
S251
暗号文を受信
S753
暗号側の公開情報
(鍵用、IV用)の読み出し
S757
復号の時に、
KPSに従い共通鍵
およびIVを生成
S755
Decrypt
(暗号文、暗号側の鍵用公開情報、
IV用公開情報)
S759
共通鍵およびIVで
暗号文を復号して、
平文を生成
復号側CPUに
共通鍵およびIV
はロードされない
S261
共通鍵
Decrypt
(平文、ステータス)
S763
復号側のTPMから
復号文(=平文)を入手する
共通鍵およびIVを破棄

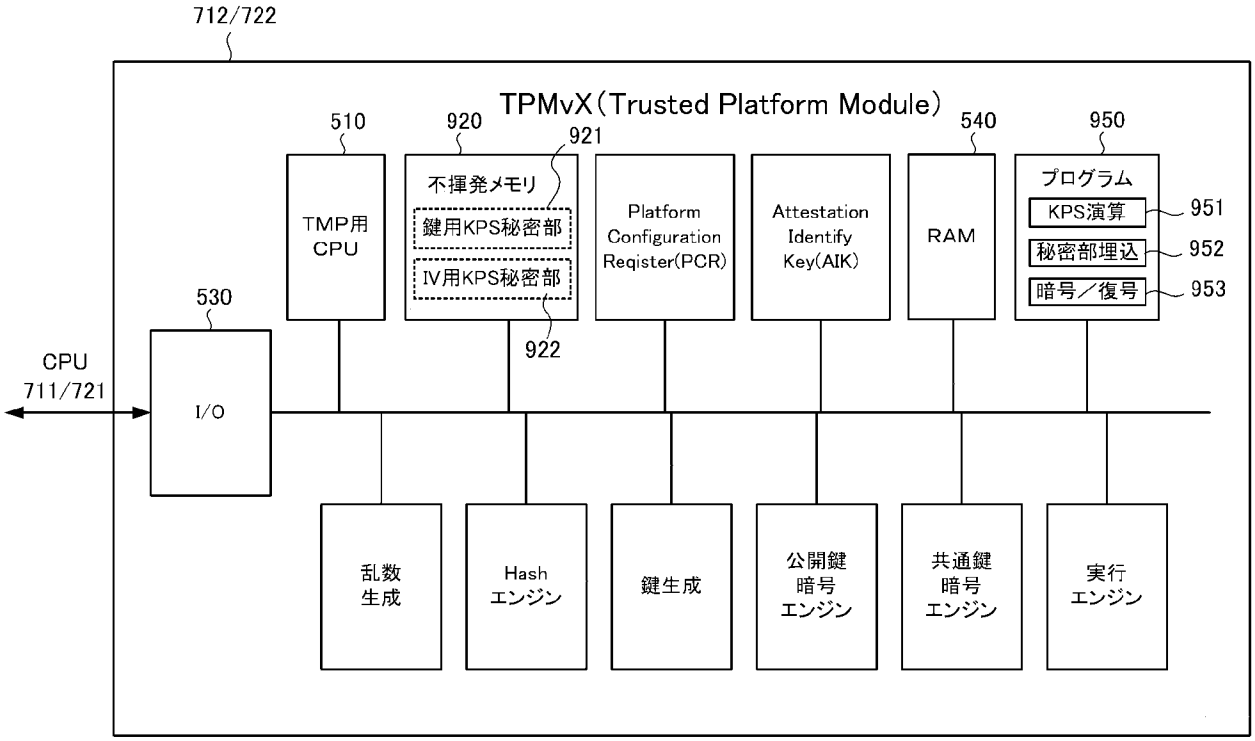
[図8A]


710, 720
360
361
表示部
362
操作部
712/722
TPM
入出力インターフェース
711/721
CPU
320
ROM
430
通信制御部
通信相手
340
RAM
平文
平文からの暗号化文
受信した暗号文
暗号文から復号した平文
送受信データ
入出力データ
850
ストレージ
通信相手の
鍵用公開情報保持部
851
通信相手の
IV用公開情報保持部
852
通信装置制御プログラム
KPS秘密部埋込モジュール
KPS公開部伝送モジュール
暗号文送信モジュール
平文復号モジュール

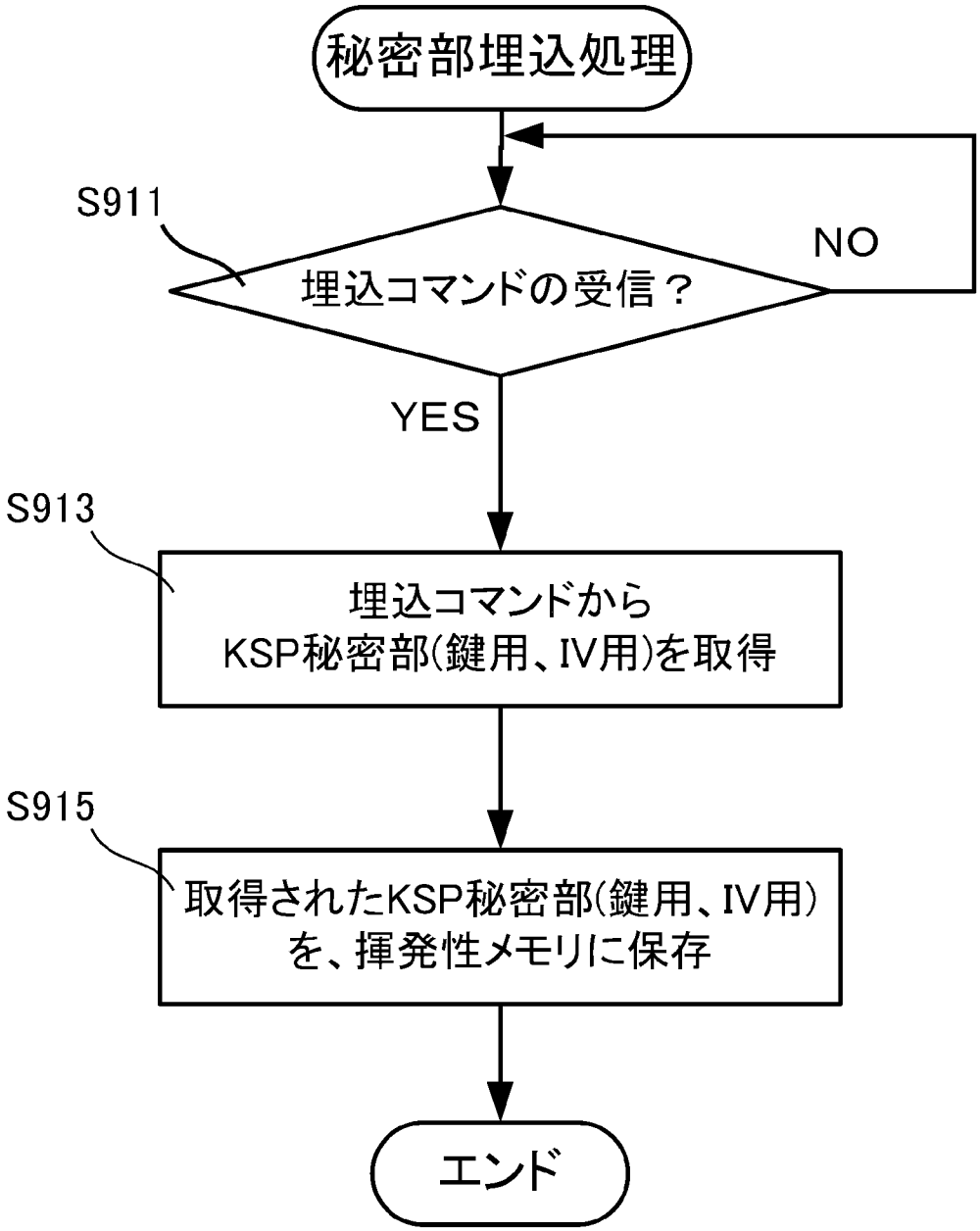
[図8B]


運用準備処理
S811
KPS(公開部，秘密部)の組
を取得
S813
TPMに、KPS秘密部(鍵用、IV用)を
埋込指示
S815
通信相手のCPUに
KPS公開部(鍵用、IV用)を伝送
S817
通信相手からの
KPS公開部を受信？
NO
YES
S819
受信した通信相手の
KPS公開部鍵用、IV用)を記憶
エンド

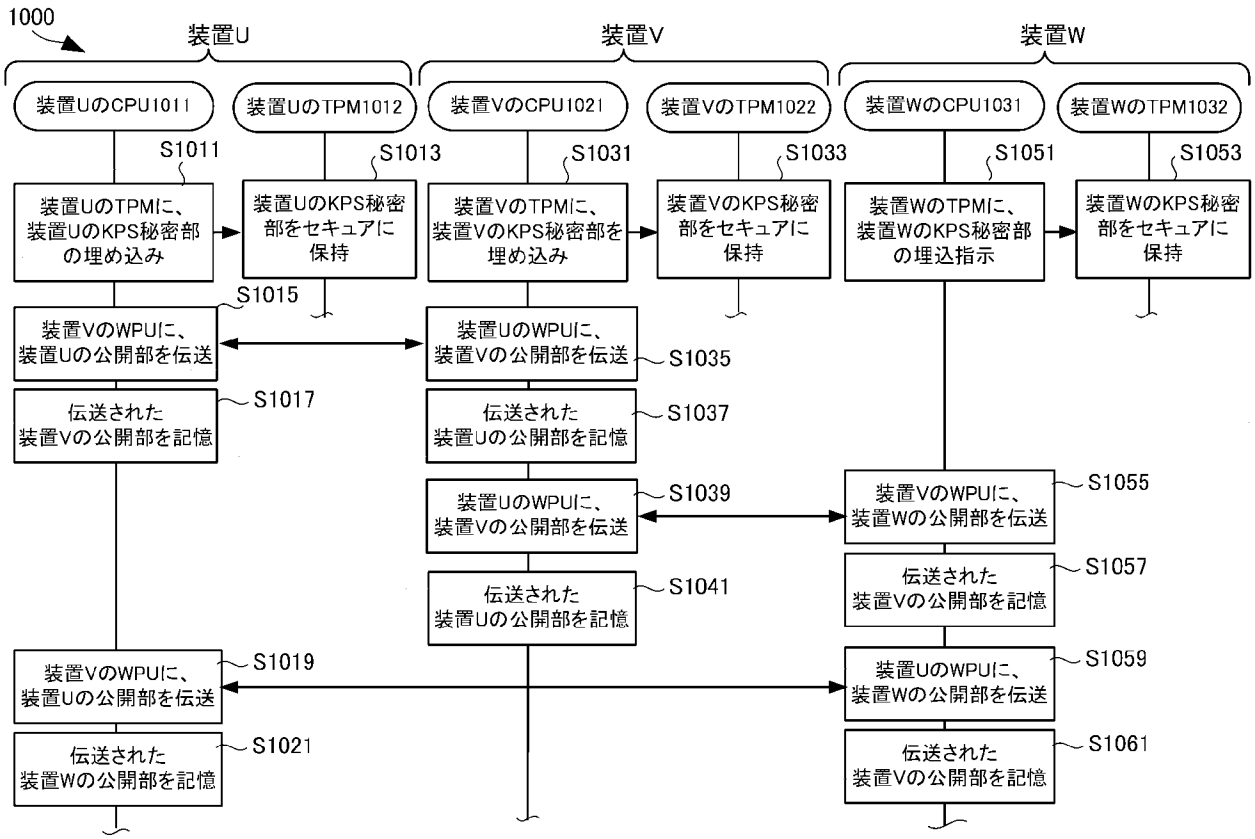
[図9A]


712/722
TPMvX(Trusted Platform Module)
510
TMP用
CPU
920
921
不揮発メモリ
鍵用KPS秘密部
IV用KPS秘密部
922
Platform
Configuration
Reqister(PCR)
Attestation
Identify
Key(AIK)
540
RAM
950
プログラム
KPS演算
951
秘密部埋込
952
暗号／復号
953
530
CPU
711/721
I/O
乱数
生成
Hash
エンジン
鍵生成
公開鍵
暗号
エンジン
共通鍵
暗号
エンジン
実行
エンジン

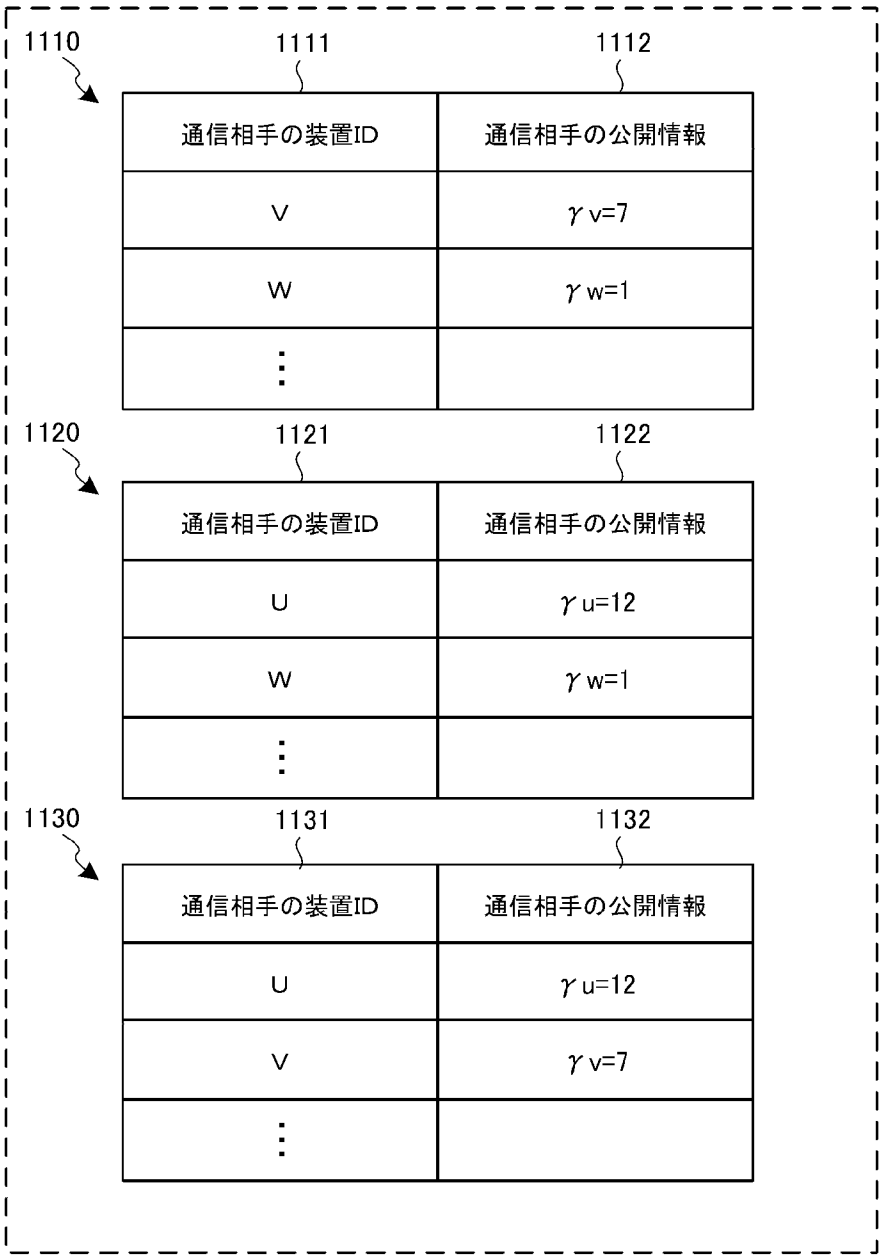
[図9B]


秘密部埋込処理
S911
埋込コマンドの受信？
NO
YES
S913
埋込コマンドから
KSP秘密部(鍵用、IV用)を取得
S915
取得されたKSP秘密部(鍵用、IV用)
を、揮発性メモリに保存
エンド

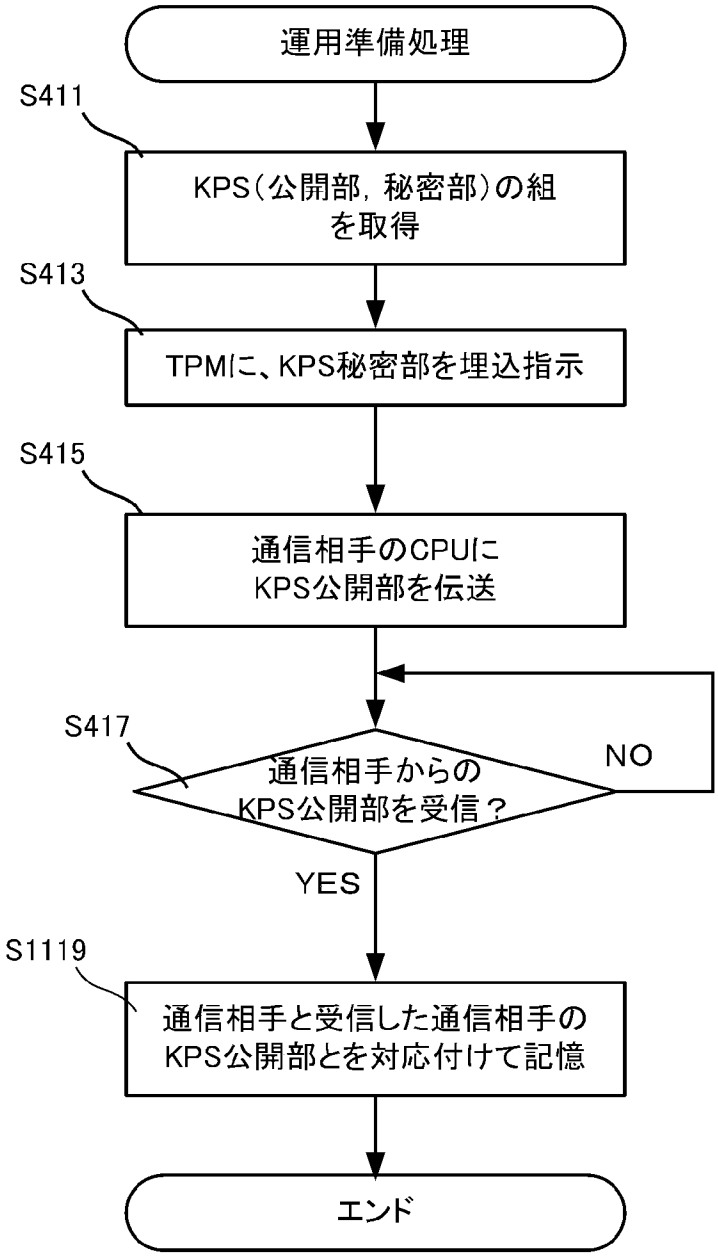
[図10]


1000
装置U
装置V
装置W
装置UのCPU1011
装置UのTPM1012
装置VのCPU1021
装置VのTPM1022
装置WのCPU1031
装置WのTPM1032
S1011
装置UのTPMに、装置UのKPS秘密部の埋め込み
S1013
装置UのKPS秘密部をセキュアに保持
S1031
装置VのTPMに、装置VのKPS秘密部を埋め込み
S1033
装置VのKPS秘密部をセキュアに保持
S1051
装置WのTPMに、装置WのKPS秘密部の埋込指示
S1053
装置WのKPS秘密部をセキュアに保持
S1015
装置VのWPUに、装置Uの公開部を伝送
装置UのWPUに、装置Vの公開部を伝送
S1035
S1017
伝送された装置Vの公開部を記憶
伝送された装置Uの公開部を記憶
S1037
装置UのWPUに、装置Vの公開部を伝送
S1039
装置VのWPUに、装置Wの公開部を伝送
S1055
伝送された装置Uの公開部を記憶
S1041
伝送された装置Vの公開部を記憶
S1057
S1019
装置VのWPUに、装置Uの公開部を伝送
装置UのWPUに、装置Wの公開部を伝送
S1059
S1021
伝送された装置Wの公開部を記憶
伝送された装置Vの公開部を記憶
S1061

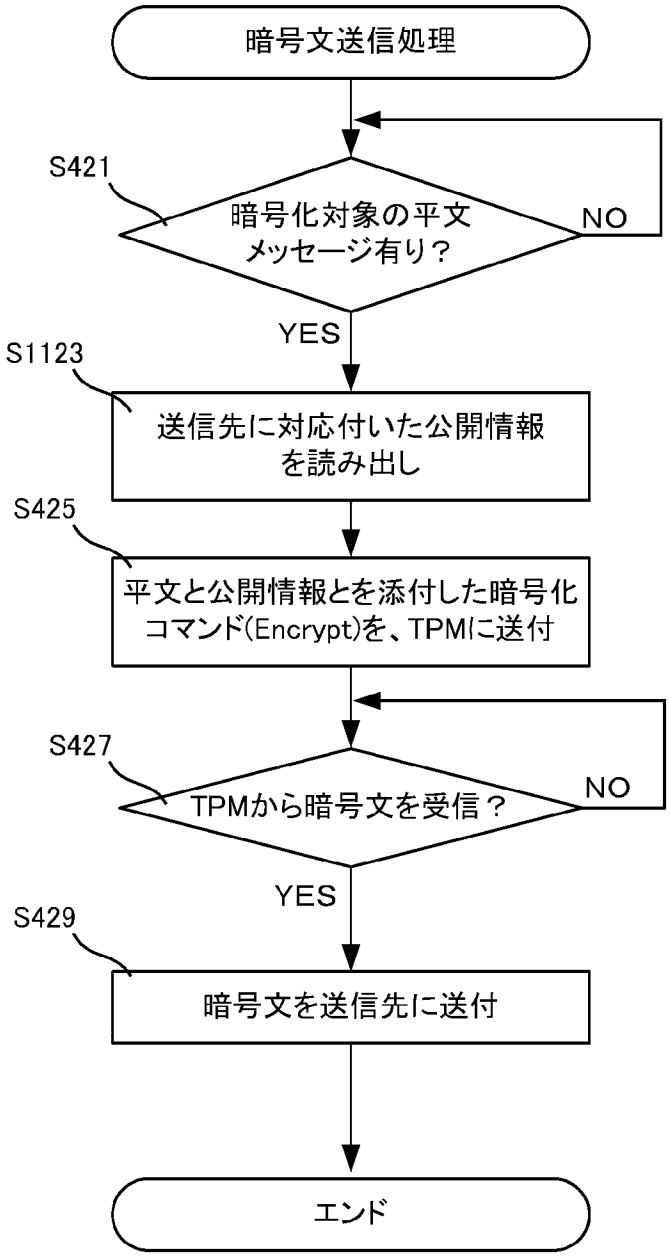
[図11A]


1110
1111
1112
通信相手の装置ID
通信相手の公開情報
V
γv=7
W
γw=1
1120
1121
1122
通信相手の装置ID
通信相手の公開情報
U
γu=12
W
γw=1
1130
1131
1132
通信相手の装置ID
通信相手の公開情報
U
γu=12
V
γv=7

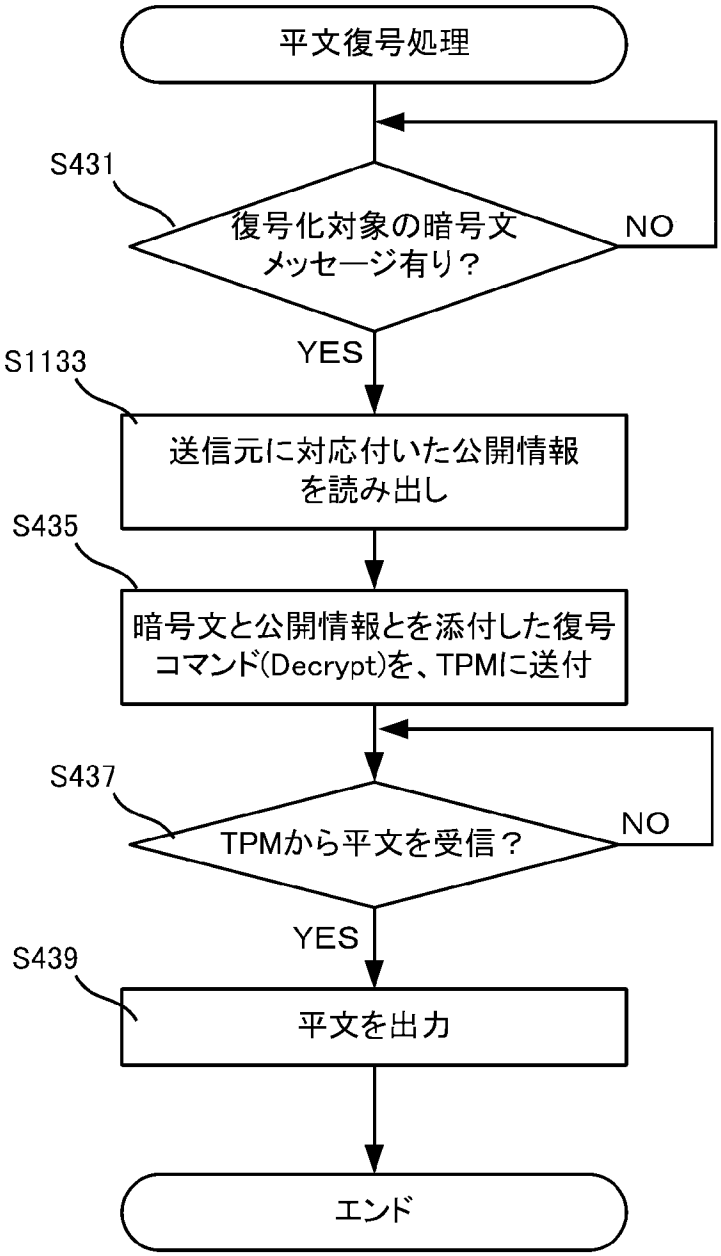
[図11B]


運用準備処理
S411
KPS(公開部，秘密部)の組を取得
S413
TPMに、KPS秘密部を埋込指示
S415
通信相手のCPUにKPS公開部を伝送
S417
通信相手からのKPS公開部を受信？
NO
YES
S1119
通信相手と受信した通信相手のKPS公開部とを対応付けて記憶
エンド

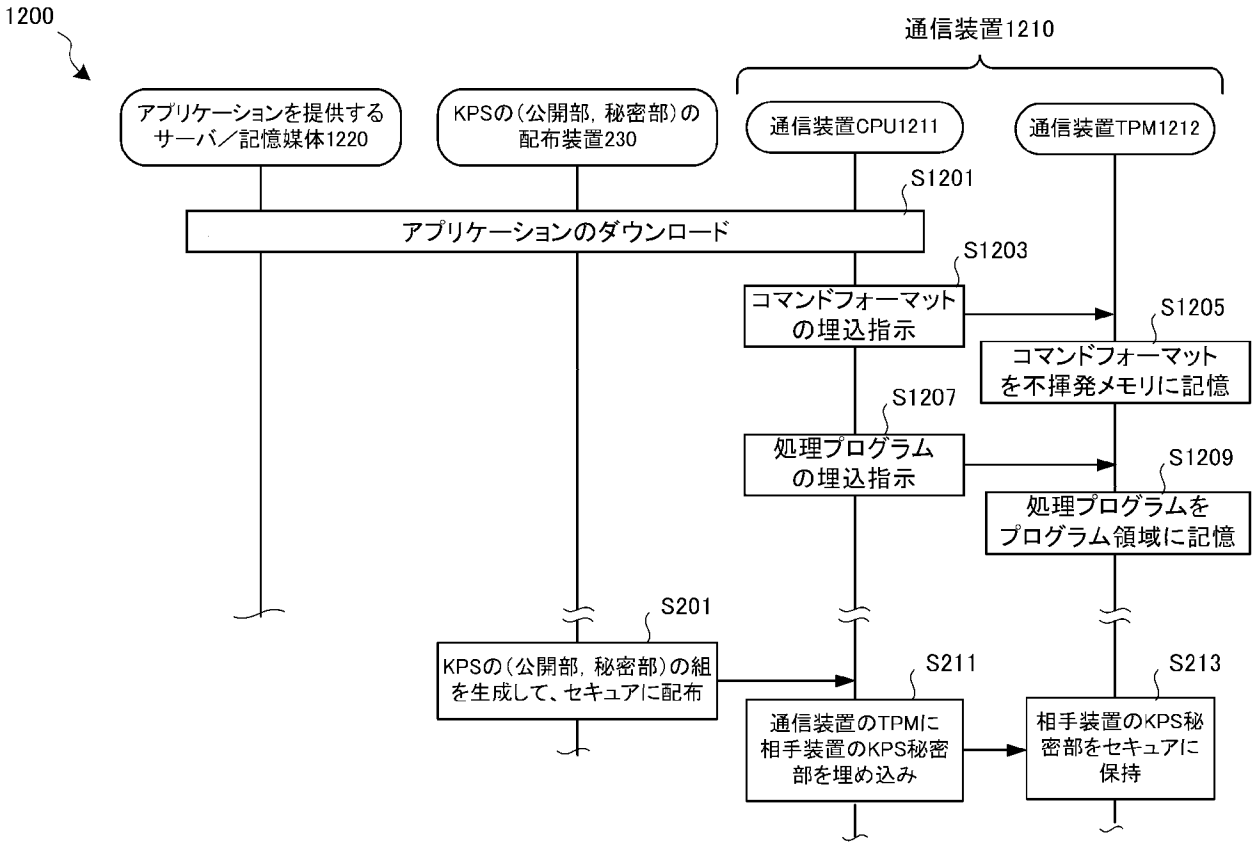
[図11C]


暗号文送信処理
S421
暗号化対象の平文
メッセージ有り？
NO
YES
S1123
送信先に対応付いた公開情報
を読み出し
S425
平文と公開情報とを添付した暗号化
コマンド(Encrypt)を、TPMに送付
S427
TPMから暗号文を受信？
NO
YES
S429
暗号文を送信先に送付
エンド

[図11D]


平文復号処理
S431
復号化対象の暗号文
メッセージ有り？
NO
YES
S1133
送信元に対応付いた公開情報
を読み出し
S435
暗号文と公開情報とを添付した復号
コマンド(Decrypt)を、TPMに送付
S437
TPMから平文を受信？
NO
YES
S439
平文を出力
エンド

[図12]


1200
通信装置1210
アプリケーションを提供するサーバ／記憶媒体1220
KPSの（公開部，秘密部）の配布装置230
通信装置CPU1211
通信装置TPM1212
S1201
アプリケーションのダウンロード
S1203
コマンドフォーマットの埋込指示
S1205
コマンドフォーマットを不揮発メモリに記憶
S1207
処理プログラムの埋込指示
S1209
処理プログラムをプログラム領域に記憶
S201
KPSの（公開部，秘密部）の組を生成して、セキュアに配布
S211
通信装置のTPMに相手装置のKPS秘密部を埋め込み
S213
相手装置のKPS秘密部をセキュアに保持

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/005311

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *H04L9/10*(2006.01)i, *H04L9/14*(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, H04L9/10, H04L9/14

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 1996-2017
Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017

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 9-238132 A (Oki Electric Industry Co., Ltd.), 09 September 1997 (09.09.1997), paragraphs [0007] to [0011], [0018]; fig. 1 & US 6018581 A column 5, line 14 to column 8, line 17; fig. 1 & EP 793367 A2 & CN 1211776 A & TW 335581 B	1-21
Y	JP 2012-506658 A (Gemalto SA), 15 March 2012 (15.03.2012), claim 11; paragraph [0005] & JP 2014-197222 A & JP 2017-34713 A & US 2011/0274268 A1 paragraph [0005] & WO 2010/046251 A1 & EP 2180631 A1 & KR 10-2011-0088509 A	1-21

☒ 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
01 May 2017 (01.05.17)	16 May 2017 (16.05.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/005311

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 2010-508576 A (Hewlett-Packard Development Co., L.P.), 18 March 2010 (18.03.2010), paragraphs [0014] to [0015]; fig. 1A to 1B & JP 4884535 B2 & US 2008/0104706 A1 paragraphs [0019] to [0020]; fig. 1A to 1B & WO 2008/054798 A1 & DE 112007002566 B & KR 10-2009-0079917 A	1-21
Y	JP 2015-233201 A (Panasonic Intellectual Property Management Co., Ltd.), 24 December 2015 (24.12.2015), paragraph [0026] (Family: none)	2,7,9,13,17, 19,21
Y	JP 2014-50038 A (West Japan Railway Co.), 17 March 2014 (17.03.2014), paragraph [0032]; fig. 5 (Family: none)	4
E,X	JP 2017-60031 A (KDDI Corp.), 23 March 2017 (23.03.2017), paragraphs [0019] to [0023], [0023], [0081] to [0087]; fig. 9 (Family: none)	8,10,12, 14-16,20

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／００５３１１

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, H04L9/10(2006.01)i, H04L9/14(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, H04L9/10, H04L9/14

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	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７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 9-238132 A（沖電気工業株式会社）1997.09.09, 段落［０００７］－［００１１］、［００１８］、［図１］ & US 6018581 A, 第５欄第１４行－第８欄第１７行、Ｆｉｇ．１ & EP 793367 A2 & CN 1211776 A & TW 335581 B	1-21
Y	JP 2012-506658 A（ジエマルト・エス・アー）2012.03.15, ［請求項１１］、段落［０００５］ & JP 2014-197222 A & JP 2017-34713 A & US 2011/0274268 A1, 段落［０００５］ & WO 2010/046251 A1 & EP 2180631 A1 & KR 10-2011-0088509 A	1-21

☑ 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
０１．０５．２０１７	１６．０５．２０１７

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　４２２９
青木　重徳
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 2010-508576 A（ヒューレットーパッカード　デベロップメントカンパニー　エル．　ピー．）2010.03.18, 段落［００１４］－［００１５］、[図１Ａ］－［図１Ｂ］ & JP 4884535 B2 & US 2008/0104706 A1, 段落［００１９］－［００２０］、ＦＩＧ．１Ａ－１Ｂ & WO 2008/054798 A1 & DE 112007002566 B & KR 10-2009-0079917 A	1-21
Ｙ	JP 2015-233201 A（パナソニックＩＰマネジメント株式会社）2015.12.24, 段落［００２６］（ファミリーなし）	2,7,9,13,17,19,21
Ｙ	JP 2014-50038 A（西日本旅客鉄道株式会社）2014.03.17, 段落［００３２］、[図５］（ファミリーなし）	4
Ｅ，Ｘ	JP 2017-60031 A（ＫＤＤＩ株式会社）2017.03.23, 段落［００１９］－［００２３］、［００２３］、 ［００８１］－［００８７］、[図９］（ファミリーなし）	8,10,12,14-16,20