(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
2014 年 1 月 9 日(09.01.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/007347 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/20* (2006.01)

(21) 国際出願番号: PCT/JP2013/068419

(22) 国際出願日: 2013 年 7 月 4 日(04.07.2013)

(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 2012-151835 2012 年 7 月 5 日(05.07.2012) JP

(71) 出願人: 株式会社クリプト・ベーシック (CRYPTO BASIC CORPORATION) [JP/JP]; 〒2130004 神奈川県川崎市高津区諏訪 3-18-40 3 階ルーム１ Kanagawa (JP).

(72) 発明者: 大矢 雅則(OYA, Masanori); 〒1628601 東京都新宿区神楽坂一丁目３番地 学校法人東京理科大学内 Tokyo (JP). 入山 聖史(IRIYAMA, Satoshi); 〒1628601 東京都新宿区神楽坂一丁目３番地 学校法人東京理科大学内 Tokyo (JP). アカルディ ルイジ(ACCARDI, Luige); 00191 ヴィア ヴィンチェンツォ チベリオ １８、ローマ Rome (IT). レゴリ マッシモ(REGOLI, Massimo); 00044 ヴィア フォンターナ ヴェッチア １８、ローマ Rome (IT).

(74) 代理人: 中島 淳, 外(NAKAJIMA, Jun et al.); 〒1600022 東京都新宿区新宿４丁目３番１７号 ＨＫ新宿ビル７階 太陽国際特許事務所 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

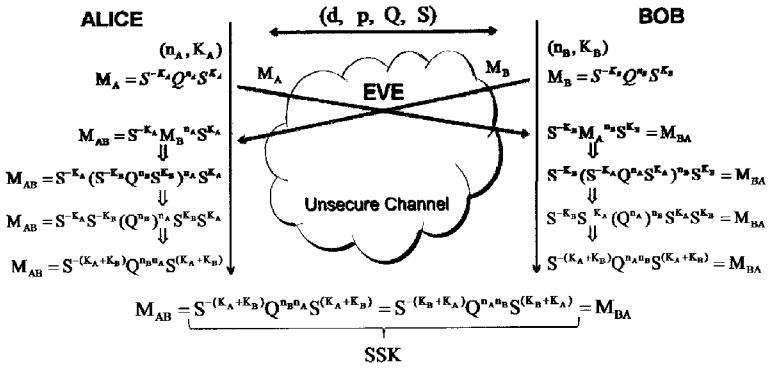
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,

[続葉有]

(54) **Title**: SHARED SECRET KEY GENERATION DEVICE, ENCRYPTION DEVICE, DECRYPTION DEVICE, SHARED SECRET KEY GENERATION METHOD, ENCRYPTION METHOD, DECRYPTION METHOD, AND PROGRAM

(54) 発明の名称 : 共有秘密鍵生成装置、暗号化装置、復号化装置、共有秘密鍵生成方法、暗号化方法、復号化方法、及びプログラム

[図3]



(57) **Abstract**: A public data acquisition section (22) acquires public data that includes a prime number p, a natural number d, a matrix Q, and a matrix S. A secret key generation section (24) generates a secret key that includes natural numbers n_A and k_A. A non-commutative matrix generation section (26) calculates a matrix M_A ($M_A = S^{-kA}Q^{nA}S^{kA}$), sends the matrix to a communication partner, and acquires a matrix M_B ($M_B = S^{-kB}Q^{nB}S^{kB}$) from the communication partner. A shared secret key calculation section (28) calculates a matrix M_{AB} ($M_{AB} = S^{-kA}M_B{}^{nA}Sk^A$) as a shared secret key. As a result, the encryption and decryption device can quickly generate a secure shared secret key.

(57) 要約: 公開データ取得部（２２）によって、素数ｐ、自然数ｄ、行列Ｑ、及び行列Ｓを含む公開データを取得し、秘密鍵生成部（２４）によって、自然数ｎ$_A$、ｋ$_A$を含む秘密鍵を生成する。非可換行列生成部（２６）によって、行列Ｍ$_A$（Ｍ$_A$＝Ｓ$^{-kA}$Ｑ^{nA}Ｓ^{kA}）を計算し、通信相手へ送信し、通信相手から行列Ｍ$_B$（Ｍ$_B$＝Ｓ$^{-kB}$Ｑ^{nB}Ｓ^{kB}）を取得する。共有秘密鍵算出部（２８）によって、行列Ｍ$_{AB}$（Ｍ$_{AB}$＝Ｓ$^{-kA}$Ｍ$_B{}^{nA}$Ｓｋ^A）を共有秘密鍵として算出する。これにより、暗号復号装置は、高速に、安全な共有秘密鍵を生成することができる。

WO 2014/007347 A1

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).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

共有秘密鍵生成装置、暗号化装置、復号化装置、共有秘密鍵生成方法、暗号化方法、復号化方法、及びプログラム

技術分野

[0001] 本発明は、共有秘密鍵生成装置、暗号化装置、復号化装置、共有秘密鍵生成方法、暗号化方法、復号化方法、及びプログラムに関する。

背景技術

[0002] 従来より、メッセージの公開型且つ非可換性の符号化方法及び暗号化方法が知られている（特開2001-202010号公報）。また、有限非可換群を用いた公開鍵暗号システムや、非可換体である環Ｒを用いた公開鍵暗号システムが知られている（特表2004-534971号公報、特表2000-516733号公報）。

[0003] また、公開鍵暗号方式によるネットワーク上での相互認証および公開鍵の相互交換システムや、制御ベクトルに基づく公開鍵暗号システムの鍵管理が知られている（特開2006-262425号公報、特開平5-216409号公報）。

発明の開示

発明が解決しようとする課題

[0004] 本発明は、高速に、安全な共有秘密鍵を生成することができる共有秘密鍵生成装置、暗号化装置、復号化装置、共有秘密鍵生成方法、暗号化方法、復号化方法、及びプログラムを提供することを目的とする。

課題を解決するための手段

[0005] 上記の目的を達成するために第１の態様に係る共有秘密鍵生成装置は、素数ｐ、自然数ｄ、行列式の値が１ではないｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を含む公開データを設定する公開データ設定部と、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成する秘密鍵生成部と、前記秘密鍵を用いて、以下の（Ｉ）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信相手へ送信する

行列計算部と、前記通信相手の秘密鍵に含まれる自然数n_B（ｍｏｄ　ｐ）、k_B（ｍｏｄ　ｐ）を用いて以下の（ＩＩ）式に従って計算される、ｄ×ｄの行列M_B（ｍｏｄ　ｐ）を取得する行列取得部と、前記行列取得部によって取得された行列MBを用いて、以下の（ＩＩＩ）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を共有秘密鍵として算出する共有秘密鍵算出部と、を含んで構成されている。

[0006] $M_A = S^{-kA} Q^{nA} S^{kA}$　　・・・（Ｉ）

$M_B = S^{-kB} Q^{nB} S^{kB}$　　・・・（ＩＩ）

$M_{AB} = S^{-kA} M_B^{nA} S^{kA}$　　・・・（ＩＩＩ）

[0007] 第２の態様に係るプログラムは、コンピュータを、素数ｐ、自然数ｄ、行列式の値が１ではないｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を含む公開データを設定する公開データ設定部、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成する秘密鍵生成部、前記秘密鍵を用いて、以下の（ＩＶ）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信相手へ送信する行列計算部、前記通信相手の秘密鍵に含まれる自然数n_B（ｍｏｄ　ｐ）、k_B（ｍｏｄ　ｐ）を用いて以下の（Ｖ）式に従って計算される、ｄ×ｄの行列M_B（ｍｏｄ　ｐ）を取得する行列取得部、及び前記行列取得部によって取得された行列M_Bを用いて、以下の（ＶＩ）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を共有秘密鍵として算出する共有秘密鍵算出部として機能させるためのプログラムである。

[0008] $M_A = S^{-kA} Q^{nA} S^{kA}$　　・・・（ＩＶ）

$M_B = S^{-kB} Q^{nB} S^{kB}$　　・・・（Ｖ）

$M_{AB} = S^{-kA} M_B^{nA} S^{kA}$　　・・・（ＶＩ）

[0009] このように、公開データと秘密鍵を用いて計算した行列を、通信相手と交換し、通信相手から得られた行列を用いて、共有秘密鍵を算出することにより、高速に、安全な共有秘密鍵を生成することができる。

[0010] 第３の態様に係る秘密鍵生成部は、前記通信相手との通信毎に、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成して更新するように

することができる。これによって、より安全な共有秘密鍵を生成することができる。

[0011] また、第４の態様に係る暗号化装置は、復号化装置と共通に設定された、請求項１又は２の共有秘密鍵生成装置によって生成された共有秘密鍵M_{AB}、及び２つの素数ｐ１、ｐ２に基づいて、２つの非可換行列Ａ１、Ａ２を生成する行列生成部と、前記復号化装置と共通に設定されたｄ次元の初期ベクトルv_0又は前回求められたｄ次元のベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1を求めると共に、前記初期ベクトルv_0、又は前回求められたｄ次元のベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、ベクトルv_i^2を求める行列作用部であって、前記非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、予め定められた、複数種類の演算子を組み合わせた演算方法に置換して、非可換行列Ａ１、Ａ２を作用させる行列作用部と、前記行列作用部によって求められたベクトルv_i^1に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ１に結合させて前記ビット列Ｗ１を求めると共に、ベクトルv_i^2に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ２に結合させて前記ビット列Ｗ２を求めるビット列変換部と、前記ビット列変換部によって求められた前記ビット列Ｗ１及び前記ビット列Ｗ２の各々のビット数が、暗号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すビット数判定部と、前記ビット列Ｗ１及び前記ビット列Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求める擬似乱数列発生部と、前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記暗号化対象データを表わすビット列との排他的論理和を計算することにより、前記暗号化対象データを暗号化する暗号化部と、を含んで構成されている。

[0012] このように、非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、複数種類の演算子を組み合わせた演算方法に置換して、ベクトルに、非可換行列Ａ１、Ａ２を繰り返し作用させると共に非線形変換

を行って、得られるビット列Ｗ１、Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求める。擬似乱数ビット列を用いて暗号化することにより、暗号化対象データのビット数が可変である場合において、暗号化処理を高速化し、かつ暗号解読強度を強くすることができる。

[0013] 第５の態様の暗号化装置に係る行列作用部は、前記初期ベクトルv_0、又は前回求められたベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、前記ベクトルv_i^1を求める際に、ベクトルv_i^1の要素毎に、既に計算されたベクトルv_i^1の要素に置き換えた前記初期ベクトルv_0又は前記ベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1の前記要素を計算し、前記初期ベクトルv_0、又は前回求められたベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、前記ベクトルv_i^2を求める際に、ベクトルv_i^2の要素毎に、既に計算されたベクトルv_i^2の要素に置き換えた前記初期ベクトルv_0又は前記ベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、ベクトルv_i^2の前記要素を計算するようにすることができる。これによって、暗号解読強度をより強くすることができる。

[0014] 第６の態様の暗号化装置に係るビット列変換部は、前記非線形変換として、前記行列作用部によって求められたベクトルv_i^1をビット列に変換し、変換されたビット列に対して、予め定められた条件を満たす先頭ビット列をカットするカットオフ処理を行い、前記先頭ビット列がカットされた前記ビット列を前回求められたビット列Ｗ１に結合させると共に、ベクトルv_i^2をビット列に変換し、変換されたビット列に対して、前記カットオフ処理を行い、前記先頭ビット列がカットされた前記ビット列を前回求められたビット列Ｗ２に結合させるようにすることができる。これによって、暗号解読強度をより強くすることができる。

[0015] また、第７の態様に係る暗号化装置のビット列変換部は、前記カットオフ処理として、前記変換されたビット列に対して、前記予め定められた条件を満たす先頭ビット列として、先頭から連続する０と、先頭から最初に出現する１とからなる先頭ビット列をカットすると共に、前記先頭ビット列がカットされた前記ビット列から、予め定められたビット数の先頭ビット列をカッ

トする処理を行うようにすることができる。これによって、暗号解読強度をより強くすることができる。

[0016] 第８の態様に係る復号化装置は、暗号化装置と共通に設定された、請求項１又は２の共有秘密鍵生成装置によって生成された共有秘密鍵M_{AB}、及び２つの素数ｐ１、ｐ２に基づいて、２つの非可換行列Ａ１、Ａ２を生成する行列生成部と、前記暗号化装置と共通に設定されたｄ次元の初期ベクトルv_0又は前回求められたｄ次元のベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1を求めると共に、前記初期ベクトルv_0、又は前回求められたｄ次元のベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、ベクトルv_i^2を求める行列作用部であって、前記非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、予め定められた、複数種類の演算子を組み合わせた演算方法に置換して、非可換行列Ａ１、Ａ２を作用させる行列作用部と、前記行列作用部によって求められたベクトルv_i^1に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ１に結合させて前記ビット列Ｗ１を求めると共に、ベクトルv_i^2に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ２に結合させて前記ビット列Ｗ２を求めるビット列変換部と、前記ビット列変換部によって求められた前記ビット列Ｗ１及び前記ビット列Ｗ２の各々のビット数が、復号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すビット数判定部と、前記ビット列Ｗ１及び前記ビット列Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求める擬似乱数列発生部と、前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記復号化対象データを表わすビット列との排他的論理和を計算することにより、前記復号化対象データを復号化する復号化部と、を含んで構成されている。

発明の効果

[0017] 本発明の一態様である共有秘密鍵生成装置、方法、及びプログラムによれば、公開データと秘密鍵を用いて計算した行列を、通信相手と交換し、通信

相手から得られた行列を用いて、共有秘密鍵を算出することにより、高速に、安全な共有秘密鍵を生成することができる。

[0018] 本発明の一態様である暗号化装置、暗号化方法、復号化装置、及び復号化方法によれば、非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、複数種類の演算子を組み合わせた演算方法に置換して、ベクトルに、非可換行列Ａ１、Ａ２を繰り返し作用させると共に非線形変換を行って、得られるビット列Ｗ１、Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求め。擬似乱数ビット列を用いて暗号化又は復号化することにより、暗号化対象データ又は復号化対象データのビット数が可変である場合において、暗号化処理又は復号化処理を高速化し、かつ暗号解読強度を強くすることができる。

図面の簡単な説明

[0019] [図1]本発明の実施の形態に係る暗号化処理システムの構成を示す概略図である。

[図2]本発明の実施の形態に係る暗号復号装置の構成を示す概略図である。

[図3]共有秘密鍵を算出する方法を説明するための図である。

[図4A]暗号化方法を説明するための図である。

[図4B]復号化方法を説明するための図である。

[図5]本発明の実施の形態に係る暗号復号装置における共有秘密鍵算出処理ルーチンの内容を示すフローチャートである。

[図6]本発明の実施の形態に係る暗号復号装置における擬似乱数列発生処理ルーチンの内容を示すフローチャートである。

[図7]コンピュータ上での実験結果を示すグラフである。

[図8]モバイル端末上での実験結果を示すグラフである。

発明を実施するための最良の形態

[0020] 以下、図面を参照して本発明の実施の形態を詳細に説明する。

[0021] ＜システム構成＞

図１に示すように、本発明の実施の形態に係る暗号化処理システム１０は

、暗号復号装置１２Ａ、１２Ｂと、複数のユーザ端末１４Ａと、複数のユーザ端末１４Ｂと、インターネットアクセス網１６とを備えている。なお、暗号復号装置１２Ａ、１２Ｂは、暗号化装置、復号化装置の一例である。

[0022] 複数のユーザ端末１４Ａは、暗号復号装置１２Ａと接続されており、暗号復号装置１２Ａは、インターネットアクセス網１６に接続されている。また、複数のユーザ端末１４Ｂは、暗号復号装置１２Ｂと接続されており、暗号復号装置１２Ｂは、インターネットアクセス網１６に接続されている。暗号復号装置１２Ａ、１２Ｂは、インターネットアクセス網１６を介して相互に接続されている。

[0023] ユーザ端末１４Ａは、インターネットアクセス網１６を介したデータ送信を行う場合に、暗号復号装置１２Ａを介して、送信データがインターネットアクセス網１６に出力される。一方、ユーザ端末１４Ａがインターネットアクセス網１６を介したデータ受信を行う場合に、暗号復号装置１２Ａを介して、受信データがインターネットアクセス網１６から入力される。

[0024] また、ユーザ端末１４Ｂは、インターネットアクセス網１６を介したデータ送信を行う場合に、暗号復号装置１２Ｂを介して、送信データがインターネットアクセス網１６へ出力される。一方、ユーザ端末１４Ｂがインターネットアクセス網１６を介したデータ受信を行う場合に、暗号復号装置１２Ｂを介して、受信データがインターネットアクセス網１６から入力される。

[0025] 暗号復号装置１２Ａ、１２Ｂは、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）と、後述する共有秘密鍵生成処理ルーチン及び擬似乱数列発生処理ルーチンを実行するためのプログラムを記憶したＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）とを備えたコンピュータで構成され、機能的には次に示すように構成されている。図２に示すように、暗号復号装置１２Ａ、１２Ｂは、通信部２０、公開データ取得部２２、秘密鍵生成部２４、非可換行列生成部２６、共有秘密鍵算出部２８、データ入出力部３２、共通データ設定部３４、擬似乱数列発生部３６、暗号化部３８、及び復号化部４０を備えている

。なお、非可換行列生成部２６は、行列計算部の一例であり、共有秘密鍵算出部２８は、行列取得部及び共有秘密鍵算出部の一例である。また、擬似乱数列発生部３６は、行列生成部、行列作用部、ビット列変換部、ビット数判定部、及び擬似乱数発生列部の一例である。

[0026] 通信部２０は、インターネットアクセス網１６を介してデータの送受信を行う。

[0027] データ入出力部３２は、ユーザ端末１４Ａ、１４Ｂから出力されたデータが入力されると共に、ユーザ端末１４Ａ、１４Ｂに対してデータを出力する。

[0028] 暗号復号装置１２Ａ、１２Ｂの公開データ取得部２２は、通信部２０を介して、通信相手との通信で用いる公開データとして、素数ｐ、自然数ｄ、ｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を取得する。ただし、ｄｅｔ　Ｑ≠１であり、（ｍｏｄ　ｐ）は、変数あるいは行列の要素の値が、素数ｐの法であることを示す。

[0029] 暗号復号装置１２Ａの秘密鍵生成部２４は、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）からなる秘密鍵を生成する。

[0030] 暗号復号装置１２Ｂの秘密鍵生成部２４は、自然数n_B（ｍｏｄ　ｐ）、k_B（ｍｏｄ　ｐ）からなる秘密鍵を生成する。

[0031] 秘密鍵生成部２４は、通信を行う毎に、新たな秘密鍵を生成し、秘密鍵を更新する。

[0032] 暗号復号装置１２Ａの非可換行列生成部２６は、秘密鍵n_A、k_Aを用いて、以下の（１）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信部２０を介して、通信相手である暗号復号装置１２Ｂへ、行列M_Aを送信する。

[0033] $$M_A = S^{-kA} Q^{nA} S^{kA} \quad \cdots (1)$$

[0034] 暗号復号装置１２Ｂの非可換行列生成部２６は、秘密鍵n_B、k_Bを用いて、以下の（２）式に従って、ｄ×ｄの行列M_B（ｍｏｄ　ｐ）を計算し、通信部２０を介して、通信相手である暗号復号装置１２Ａへ、行列MBを送信する。

[0035] $$M_B = S^{-kB} Q^{nB} S^{kB} \quad \cdots (2)$$

[0036] 暗号復号装置１２Ａの共有秘密鍵算出部２８は、通信部２０によって受信した行列M_Bを取得し、取得された行列M_Bを用いて、以下の（３）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を算出する。

[0037] $M_{AB}=S^{-kA}M_B^{nA}S^{kA}$ ・・・（３）

[0038] 暗号復号装置１２Ｂの共有秘密鍵算出部２８は、通信部２０によって受信した行列M_Aを取得し、取得された行列M_Aを用いて、以下の（４）式に従ってｄ×ｄの行列M_{BA}（ｍｏｄ　ｐ）を算出する。

[0039] $M_{BA}=S^{-kB}M_A^{nB}S^{kB}$ ・・・（４）

[0040] ここで、図３に示すように、上記（３）式は、以下のように、（５）式に変換される。

[0041] $M_{AB}=S^{-KA}M_B^{nA}S^{KA}$

$M_{AB}=S^{-KA}(S^{-KB}Q^{nB}S^{KB})^{nA}S^{KA}$

$M_{AB}=S^{-KA}S^{-KB}(Q^{nB})^{nA}S^{KB}S^{KA}$

$M_{AB}=S^{-(KA+KB)}Q^{nBnA}S^{(KA+KB)}$ ・・・（５）

[0042] また、上記（４）式は、以下のように、（６）式に変換される。

[0043] $S^{-KB}M_A^{nB}S^{KB}=M_{BA}$

$S^{-KB}(S^{-KA}Q^{nA}S^{KA})^{nB}S^{KB}=M_{BA}$

$S^{-KB}S^{-KA}(Q^{nA})^{nB}S^{KA}S^{KB}=M_{BA}$

$S^{-(KA+KB)}Q^{nAnB}S^{(KA+KB)}=M_{BA}$ ・・・（６）

[0044] 上記（５）式、（６）式により、以下の（７）式が得られ、M_{AB}とM_{BA}とが等しいことが証明される。

[0045] $M_{AB}=S^{-(KA+KB)}Q^{nAnB}S^{(KA+KB)}=S^{-(KB+KA)}Q^{nAnB}S^{(KB+KA)}=M_{BA}$

・・・（７）

[0046] そこで、暗号復号装置１２Ａ、１２Ｂの共有秘密鍵算出部２８は、算出した行列M_{AB}、M_{BA}を、共有秘密鍵として、共通データ設定部３４へ出力する。

[0047] 共通データ設定部３４は、暗号復号装置１２Ａ、１２Ｂで共通のデータを設定する。具体的には、共有秘密鍵である行列M_{AB}（M_{BA}）、プライベートデ

ータである素数ｐ１、ｐ２、及び初期ベクトルv_0が共通のデータとして設定される。

[0048] 擬似乱数列発生部３６は、後述する手法により、共有秘密鍵である行列M_{AB}（M_{BA}）、プライベートデータである素数ｐ１、ｐ２、及び初期ベクトルv_0を用いて、擬似乱数ビット列を発生させる。

[0049] 暗号化部３８は、擬似乱数列発生部３６によって発生した擬似乱数ビット列を、ワンタイムパッド暗号の鍵として用いることで、データ入出力部３２により入力された暗号化対象データに対して、ストリーム暗号化を行う。例えば、暗号化部３８は、図４Ａに示すように、ビット列で表した平文（plain text）と、暗号化の鍵としての擬似乱数ビット列とのＸＯＲを演算することにより、前から１ビット毎に（あるいは1バイト毎に）暗号化する。暗号化部３８により暗号化されたデータは、通信部２０によりデータ送信される。

[0050] 復号化部４０は、擬似乱数列発生部３６によって発生した擬似乱数ビット列を、ワンタイムパッド暗号の鍵として用いることで、通信部２０により受信された復号化対象データに対して、復号化を行う。例えば、復号化部４０は、図４Ｂに示すように、ビット列で表した暗号化文（cypher text）と、暗号化の鍵としての擬似乱数ビット列とのＸＯＲを演算することにより、前から１ビット毎に（あるいは1バイト毎に）復号化する。復号化部４０により復号化されたデータは、データ入出力部３２により、データ端末１４Ａ、１４Ｂへ出力される。

[0051] 次に、本実施の形態における擬似乱数ビット列を発生させる原理について説明する。

[0052] まず、擬似乱数列発生部３６は、共通秘密鍵として生成されたｄ×ｄの行列M_{AB}（またはM_{BA}）及び共通のプライベートデータとして設定された素数ｐ１、ｐ２とを用いて、以下のように、２つの非可換行列Ａ１、Ａ２を生成する。なお、以下では、行列M_{AB}が、２×２の行列である場合を例に説明する。

[0053] 擬似乱数列発生部３６は、以下の（８）式に示すように、行列M_{AB}と素数ｐ１とを用いて、行列Ａ１’を計算する。

[0054] [数1]

$$A_1' \equiv M_{AB} \bmod p_1$$
$$\equiv \begin{pmatrix} a \bmod p_1 & b \bmod p_1 \\ c \bmod p_1 & d \bmod p_1 \end{pmatrix}$$
$$\equiv \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \quad \cdots (8)$$

[0055] そして、擬似乱数列発生部３６は、＜ｇ＞＝｛１，…，ｐ$_1$－１｝となるジェネレータｇを求める。例えば、ｐ$_1$＝７のジェネレータは、以下のように、＜３＞＝｛１，…，６｝である。

[0056] ３^1＝３，３^2＝９ｍｏｄ７＝２，３^3＝２７ｍｏｄ７＝６，３^4＝８１ｍｏｄ７＝４，

３^5＝２４３ｍｏｄ７＝５，・・・

[0057] そして、Ａ$_1$”を、以下の（９）式で表わすとすると、擬似乱数列発生部３６は、ｄｅｔ　Ａ$_1$”＝ｇになるようにｄ’を変更し、ｄ’を変更したＡ”$_1$を、非可換行列Ａ１とする。

[0058] [数2]

$$A_1'' \equiv \begin{pmatrix} g & b' \\ c' & d' \end{pmatrix}, \quad \cdots (9)$$

[0059] また、擬似乱数列発生部３６は、以下の（１０）式に示すように、行列M_{AB}と素数ｐ２とを用いて、行列Ａ２’を計算し、上記と同様に、非可換行列Ａ２を生成する。

[0060] [数3]

$$A_2' = M_{AB} \bmod p_2 = \begin{pmatrix} a \bmod p_2 & b \bmod p_2 \\ c \bmod p_2 & d \bmod p_2 \end{pmatrix} \quad \cdots (10)$$

[0061] ここで、非可換行列Ａ１、Ａ２を用いて生成される擬似乱数列の周期の長さＯ（Ａ）は、非可換行列Ａ１、Ａ２の生成に用いる、任意の素数ｐを用いて、以下の（１１）式のように書ける。

[0062] Ｏ（Ａ）≧ｐ　　・・・（１１）

[0063] たとえば、ｐを１００００００ビットの素数とした場合、Ａの周期はそれ以上に長くなる。

[0064] また、擬似乱数列発生部３６は、共通に設定された初期ベクトルv_0に対して、生成された非可換行列A_1を用いて変換を行い、ベクトルv_1を得る。また、ベクトルv_1に対して、非可換行列A_1を用いた変換を繰り返し、ベクトル列$V=\{v_0, v_1, \ldots, v_t\}$を得る。ここで$v_i = A_1^i v_0$である。

[0065] そして、擬似乱数列発生部３６は、得られたベクトル列Ｖから非線形変換により、ビット列Ｗ１を得る。ベクトル列Ｖからビット列Ｗを得る非線形変換として、Ｖの要素を$v_i = (v_{i,0}, v_{i,1}, \ldots, v_{i,n})$とし、$v_{i,0}$をバイナリ変換したビット列から、先頭ビットから続く０と次に現われた１とからなるビット列を含む先頭ビット列を取り除くカットオフ処理を行う。ここで、カットオフの後、残ったビット列は高い乱数性を持つことが知られている。

[0066] 本実施の形態では、カットオフ処理において、Random cut及びFixed cutの2種類のカットオフを使用している。

[0067] Random cutでは、上述したように、最初に現れる連続した0と、次に出現する1とからなる先頭ビット列をカットする。また、Fixed cutでは、あらかじ

め決めておいたビット数だけカットする。例えば、Fixed cutでカットするビット数が3である場合、Random cutの結果として得られるビット列の先頭3ビットをカットする。

[0068] v_iの要素すべてにこのカットオフ処理を行い、カットオフ処理後の要素を全て並べたビット列をWとする。

[0069] 攻撃者は、すべてのカットオフの可能性を検証しなければ、非可換行列Ａ１とＡ２を復元することはできないため、攻撃に対する強さを向上させることができる。

[0070] また、本実施の形態では、ベクトルv_iに、非可換行列Ａ１、Ａ２を作用させて、新しいベクトルv_{i+1}を得る際に、数同士の和演算及び積演算を、以下のように複数の演算子を組み合わせた演算に置き換える。

[0071] 例えば、a、bを32bitの数とし、記号a<<kを、aをkビットずらす記号とすると、（和演算）a+bを、a+b mod 2^{32}に置き換える。また、（積演算）a×b を、 a<< (b / 2^{27}) xorbに置き換える。ここで、a<< (b / 2^{27})は、a を 、bを2^{27}で割った商だけずらすことを表わし、xorはビットごとの排他的論理和を表わす。

[0072] また、ベクトルv_iに、非可換行列Ａ１、Ａ２を作用させて、新しいベクトルv_{i+1}を得る際に、更に、行列の作用の方法を以下のように置き換えてもよい。

[0073] 例えば、v_i＝（v_i^1, v_i^2,..., v_i^d）を、行列Ａを初期ベクトルv_0にi回作用させたものとする（dはＡの次元）と、v_{i+1}＝（v_{i+1}^1, v_{i+1}^2,..., v_{i+1}^d）を得る方法を以下のようにする。

[0074] まず、v_{i+1}^1＝（Ａv_i）^{1}とする。これはベクトルＡv_iの1番目の要素だけである。また、必要な計算は1番目の要素の計算だけである。2x2行列で書くと、

[0075]

[数4]

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} v \\ w \end{pmatrix} \rightarrow av + bw$$

[0076] となるが、和演算と積演算は、上述したように、別の演算で置き換えられている。

[0077] そして、$v_{i+1}^{2}=(A(v_{i+1}^{1}, v_i^{2},\ldots, v_i^{d}))^{2}$とする。これは非可換行列Ａを、$v_i$の1番目の要素を$v_{i+1}^{1}$に置き換えたものに作用させ、２番目の要素を取り出したものである。なお、ここで必要な計算は、2番目の要素の計算だけである。

[0078] そして、$v_{i+1}^{3}=(A(v_{i+1}^{1}, v_{i+1}^{2},\ldots, v_i^{d}))^{2}$とする。これは上記と同様に、$v_i$の１番目、２番目の要素を置き換えて、非可換行列Ａを作用させ、3番目の要素を抜き出したものである。

[0079] 以降、d番目の要素まで同様に行い、v_{i+1}を得る。

[0080] また、暗号化する平文のビット数をｎとすると、ビット列Ｗ１のビット数がnに到達した瞬間、ビット列Ｗ１に対する処理は中断され、ビット列Ｗ１の余った部分は捨てられる。

[0081] 擬似乱数列発生部３６は、非可換行列A_2に対しても同様に、ベクトルへの作用及びカットオフ処理を繰り返し行い、ビット列Ｗ２を生成する。また、ビット列Ｗ２のビット数がnに到達した瞬間、ビット列Ｗ２に対する処理は中断され、ビット列Ｗ２の余った部分は捨てられる。

[0082] そして、擬似乱数列発生部３６は、最終的に得られたビット列Ｗ１とビット列Ｗ２とのＸＯＲを計算し、得られたビット列を、擬似乱数ビット列とする。なお、ビット列Ｗ１とビット列Ｗ２とのＸＯＲにより得られたビット列に対して、更に非線形変換を行って、その結果を、擬似乱数ビット列として

もよい。

[0083] 擬似乱数列発生部３６は、上記のように、暗号化対象データのビット数又は復号化対象データのビット数と同じビット数の擬似乱数ビット列を発生させる。

[0084] ＜暗号化処理システムの動作＞

次に、本実施の形態に係る暗号化処理システム１０の動作について説明する。

[0085] まず、ユーザ端末１４Ａから、データをユーザ端末１４Ｂへ送信する場合に、ユーザ端末１４Ａが、送信データを、暗号復号装置１２Ａに出力する。

[0086] 次に、暗号復号装置１２Ａは、通信相手の暗号復号装置１２Ｂに対して、通信開始要求を送信し、暗号復号装置１２Ｂから応答信号を受信すると、暗号復号装置１２Ａにおいて、図５に示す共有秘密鍵算出処理ルーチンが実行される。また、暗号復号装置１２Ｂにおいても、同様に、図５に示す共有秘密鍵算出処理ルーチンが実行される。なお、以下では、暗号復号装置１２Ａにおいて、共有秘密鍵算出処理ルーチンを実行する場合について説明する。

[0087] まず、ステップ１００において、暗号復号装置１２Ａは、暗号復号装置１２Ａ、１２Ｂの間の通信において用いる公開データ（ｐ、ｄ、Ｑ、Ｓ）を取得する。例えば、Ｗｅｂ上に公開された公開データにアクセスして取得する。

[0088] そして、ステップ１０２において、暗号復号装置１２Ａは、秘密鍵n_A、k_Aを生成する。次のステップ１０４では、暗号復号装置１２Ａは、上記ステップ１００で取得した公開データと、上記ステップ１０２で生成した秘密鍵とに基づいて、上記（１）式に従って、非可換行列M_Aを算出する。

[0089] ステップ１０６では、暗号復号装置１２Ａは、上記ステップ１０４で算出した非可換行列M_Aを、通信相手の暗号復号装置１２Ｂへ送信する。次のステップ１０８では、暗号復号装置１２Ａは、暗号復号装置１２Ｂから、非可換行列M_Bを受信したか否かを判定する。暗号復号装置１２Ａは、暗号復号装置１２Ｂによって同様に算出された非可換行列M_Bを受信すると、ステップ１１

０へ進む。

[0090] ステップ１１０では、暗号復号装置１２Ａは、上記ステップ１００で取得した公開データと、上記ステップ１０２で生成した秘密鍵と、上記ステップ１０８で受信した非可換行列M_Bとに基づいて、上記（３）式に従って、行列M_{AB}を算出して、暗号復号装置１２Ｂとの通信における共有秘密鍵として設定し、共有秘密鍵算出処理ルーチンを終了する。

[0091] 上記共有秘密鍵算出処理ルーチンは、通信が開始される毎に実行され、その度に、新しい秘密鍵が生成され、新しい共有秘密鍵が設定される。

[0092] また、暗号復号装置１２Ａにおいて、図６に示す擬似乱数列発生処理ルーチンが実行される。

[0093] まず、ステップ１２０において、暗号復号装置１２Ａは、暗号復号装置１２Ｂと共通に設定された共有秘密鍵M_{AB}、素数ｐ１、ｐ２を用いて、非可換行列Ａ１、Ａ２を生成する。ステップ１２２では、暗号復号装置１２Ａは、ベクトルを識別する変数ｉを初期値である０に設定する。また、暗号復号装置１２Ａは、初期ベクトル$v0$を設定する。

[0094] 次のステップ１２４では、暗号復号装置１２Ａは、ベクトルv_iに、非可換行列Ａ１、Ａ２をそれぞれ作用させて、ベクトルv_{i+1}^1、v_{i+1}^2を計算する。ステップ１２６では、暗号復号装置１２Ａは、上記ステップ１２４で計算されたベクトルv_{i+1}^1、v_{i+1}^2の各々を、ビット列に変換すると共に、それぞれのビット列に対して、カットオフ処理を行い、先頭ビット列をカットオフする。そして、ステップ１２８において、暗号復号装置１２Ａは、上記ステップ１２６で得られたビット列の各々を、ビット列Ｗ１、Ｗ２に対して更に並べるように追加する。

[0095] ステップ１３０では、暗号復号装置１２Ａは、ビット列Ｗ１、Ｗ２の各々のビット数が、送信データ（暗号化対象データ）のビット列のビット数に到達したか否かを判定する。ビット列Ｗ１、Ｗ２の各々のビット数が、ユーザ端末１４Ａから入力された送信データ（暗号化対象データ）のビット列のビット数に到達していない場合には、ステップ１３２において、暗号復号装置

１２Ａは、変数ｉを１インクリメントして、上記ステップ１２４へ戻って、ステップ１２４以降の処理を繰り返す。ここで、ビット列Ｗ１のみについて、ビット数が、送信データのビット列のビット数に到達した場合には、上記ステップ１２４以降の処理において、非可換行列Ａ１を用いた処理は行わない。また、ビット列Ｗ２のみについて、ビット数が、送信データのビット列のビット数に到達した場合には、上記ステップ１２４以降の処理において、非可換行列Ａ２を用いた処理は行わない。

[0096] また、上記ステップ１３０において、ビット列Ｗ１、Ｗ２の双方のビット数が、送信データのビット列のビット数に到達したと判定された場合には、ステップ１３４へ進む。

[0097] ステップ１３４では、暗号復号装置１２Ａは、ビット列Ｗ１、Ｗ２のＸＯＲを演算して、擬似乱数ビット列Ｓを生成し、擬似乱数列発生処理ルーチンを終了する。

[0098] そして、暗号復号装置１２Ａは、上記の擬似乱数列発生処理ルーチンによって生成された擬似乱数ビット列Ｓと、ユーザ端末１４から入力された送信データのビット列とのＸＯＲを演算することにより、暗号化された送信データを生成する。また、暗号復号装置１２Ａは、暗号化された送信データを、インターネットアクセス網１６を介してユーザ端末１４Ｂへ送信する。

[0099] 暗号化された送信データは、暗号復号装置１２Ｂによって受信され、暗号復号装置１２Ｂにおいて、上記図６の擬似乱数列発生処理ルーチンが同様に実行され、暗号化された送信データと同じビット数の擬似乱数ビット列Ｓが生成される。

[0100] そして、暗号復号装置１２Ｂは、生成された擬似乱数ビット列Ｓと、暗号化された送信データのビット列とのＸＯＲを演算することにより、暗号化された送信データの平文を生成する。また、暗号復号装置１２Ｂは、送信データの平文を、送信先として指定されたユーザ端末Ｂへ出力する。

[0101] 次に、上記の実施の形態で説明した共有秘密鍵の算出アルゴリズムを用いた実験を行った結果について説明する。

[0102] ２者間における鍵共有の速度を検証した。秘密鍵を生成し、交換が終了するまでの計算時間を計測した。

[0103] また、以下の環境でテストを行った。Ｗｉｎｄｏｗｓ７（登録商標）上のパフォーマンスは、以下の表１に示す。

[0104] [表1]

CPU	E5300@2.6GHz Intel Pentium
RAM	4GB DDR 2 800 (vData 2x2GB)
HDD	500GB7200RPM (Western Digital Caviar Blue)
OS	MS Windows7 32-bit

（ＲＳＡ公開鍵暗号（図７のRSA参照））、Diffie-Hellman型暗号（図７のDH参照)、Elliptic Curve（楕円）暗号（図７のECC参照）を比較対象として、速度の比較を行い、鍵生成、公開情報生成、鍵共有の速度をプロットした。図７に示すグラフより、本実施の形態で提案した手法（図７のQP-kex参照）は他の方式より圧倒的に速く、特に、RSAと比較して約10倍の速度であることが分かった。

[0105] また、以下の表２に示すようなモバイル端末上で、実装実験を行った。

[0106] [表2]

CPU	TI OMAP 1710, 220MHz processor
OS	Symbian OS 8.1a, Series 60 UI operating system

この端末はNokia（Ｒ） N70 platform である。比較とする対象は、Diffie-Hellman型暗号（図８のDH参照)、Elliptic Curve（楕円）暗号（図８のECC参照） である。ＲＳＡ公開鍵暗号は非常に実行時間がかかるため割愛した。横軸に方式名と鍵長をとり、縦軸を実行時間とした。図８に示すグラフより、本実施の形態で提案した手法（図８のQP参照）は小型デバイスでも他の方式と比べ、圧倒的に実行時間が速く、鍵長を長くとっても実行時間は大きく

ならないということが分かった。

[0107] 以上説明したように、本発明の実施の形態に係る暗号復号装置は、公開データと秘密鍵を用いて計算した非可換行列を、通信相手と交換し、通信相手から得られた非可換行列を用いて、共有秘密鍵を算出することにより、高速に、安全な共有秘密鍵を生成することができる。

[0108] また、暗号復号装置は、高速な処理で、長い鍵を共有することができる。

[0109] また、共通秘密鍵への攻撃に対する強さについては、攻撃者は公開されている情報（ｐ、ｄ、Ｑ，Ｓ）と公開鍵$_{M}$Ａ、M_Bから、次の問題を解き、秘密鍵n_A、k_A、（若しくはn_B、k_B）を得る必要がある。

[0110] [問題]次を満たすn_A、k_Aを求めよ。

$M_A = S^{-K_A} Q^{n_A} S^{K_A}$

[0111] これは、ＤＨ型（離散対数問題）よりはるかに難しい問題となる。仮にn_Aを得ることができても、それからk_Aを得るには、非線形問題を解かねばならない。このとき、不定方程式が出現し、数学的には解を得る確率は０となる。従って、生成される共有秘密鍵は、D-H より数学的に厳密に安全である。

[0112] また、暗号復号装置は、非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算を、複数種類の演算子を組み合わせた演算方法に置換して、初期ベクトルに、非可換行列Ａ１、Ａ２を繰り返し作用させると共に非線形変換を行って、得られるビット列Ｗ１、Ｗ２のＸＯＲを計算して、擬似乱数ビット列を求める。暗号復号装置は、擬似乱数ビット列を用いて暗号化又は復号化することにより、暗号化対象データ又は復号化対象データのビット数が可変である場合において、暗号化処理又は復号化処理を高速化し、かつ暗号解読強度を強くすることができる。また、暗号復号装置は、共有秘密鍵の生成方法と、乱数を用いた暗号化・復号化方法とを組み合わせることで、高速かつ安全にストリーム暗号を開始することができる。

[0113] また、他のストリーム暗号より高速で、計算能力の低い小型デバイス上でも実装が可能である。

[0114] また、擬似乱数列発生アルゴリズムにおいて、いくつかの非線形変換を用

いることにより、擬似乱数列の統計的ランダム性と長周期を保証することができ、生成された擬似乱数列を用いることにより、安全な使い捨て暗号鍵（One-Time-Padキー）を生成することができる。

[0115] また、ストリーミング暗号を実現することができるため、音声・動画などのマルチメディア・ファイルを安全にかつ高速に転送することができる。

[0116] なお、本発明は、上述した実施形態に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。

[0117] 例えば、サーバとモバイルとの間の通信を行うようにしてもよい。上記の共有秘密鍵の生成方法は、モバイル環境でも高速に動作し、鍵交換を行う２者間で計算量を偏らせることができるため、サーバとモバイル間通信に適している。

[0118] また、ストリーミング暗号以外に、本発明を適用してもよく、自動車のキーレスエントリーなどへ応用してもよい。また、HDD(hard disk drive)の暗号化に応用してもよい。例えば、本実施の形態で説明した暗号化方法により、HDDに保存されるすべてのデータが暗号化され、正当なユーザしか読み出しできないようにしてもよい。また、Cloudサービスのセキュリティに、本発明を応用してもよい。

[0119] また、本願明細書中において、プログラムが予めインストールされている実施形態として説明したが、当該プログラムを、コンピュータ読み取り可能な記録媒体に格納して提供することも可能である。

[0120] 本発明の一態様のコンピュータ可読媒体は、コンピュータを、素数ｐ、自然数ｄ、行列式の値が１ではないｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を含む公開データを設定する公開データ設定部、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成する秘密鍵生成部、前記秘密鍵を用いて、以下の（ＩＶ）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信相手へ送信する行列計算部、前記通信相手の秘密鍵に含まれる自然数n_B（ｍｏｄ　ｐ）、k_B（ｍｏｄ　ｐ）を用いて以下の（Ｖ）式に従って計算される、ｄ×ｄの行列M_B（ｍｏｄ

ｐ）を取得する行列取得部、及び前記行列取得部によって取得された行列M_Bを用いて、以下の（ＶＩ）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を共有秘密鍵として算出する共有秘密鍵算出部として機能させるためのプログラムを記憶したコンピュータ可読媒体である。

$M_A = S^{-kA} Q^{nA} S^{kA}$　　・・・（ＩＶ）

$M_B = S^{-kB} Q^{nB} S^{kB}$　　・・・（Ｖ）

$M_{AB} = S^{-kA} M_B^{nA} S^{kA}$　　・・・（ＶＩ）

[0121] 日本出願２０１２－１５１８３５の開示はその全体が参照により本明細書に取り込まれる。

[0122] 本明細書に記載された全ての文献、特許出願、及び技術規格は、個々の文献、特許出願、及び技術規格が参照により取り込まれることが具体的かつ個々に記載された場合と同程度に、本明細書中に参照により取り込まれる。

請求の範囲

[請求項1] 素数ｐ、自然数ｄ、行列式の値が１ではないｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を含む公開データを設定する公開データ設定部と、

自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成する秘密鍵生成部と、

前記秘密鍵を用いて、以下の（Ｉ）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信相手へ送信する行列計算部と、

前記通信相手の秘密鍵に含まれる自然数n_B（ｍｏｄ　ｐ）、k_B（ｍｏｄ　ｐ）を用いて以下の（ＩＩ）式に従って計算される、ｄ×ｄの行列M_B（ｍｏｄ　ｐ）を取得する行列取得部と、

前記行列取得部によって取得された行列M_Bを用いて、以下の（ＩＩＩ）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を共有秘密鍵として算出する共有秘密鍵算出部と、

を含む共有秘密鍵生成装置。

$$M_A = S^{-kA} Q^{nA} S^{kA} \quad \cdots (I)$$

$$M_B = S^{-kB} Q^{nB} S^{kB} \quad \cdots (II)$$

$$M_{AB} = S^{-kA} M_B^{nA} S^{kA} \quad \cdots (III)$$

[請求項2] 前記秘密鍵生成部は、前記通信相手との通信毎に、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成して更新する請求項１記載の共有秘密鍵生成装置。

[請求項3] 復号化装置と共通に設定された、請求項１又は２の共有秘密鍵生成装置によって生成された共有秘密鍵M_{AB}、及び２つの素数ｐ１、ｐ２に基づいて、２つの非可換行列Ａ１、Ａ２を生成する行列生成部と、

前記復号化装置と共通に設定されたｄ次元の初期ベクトルv_0又は前回求められたｄ次元のベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1を求めると共に、前記初期ベクトルv_0、又は前回求められたｄ次元のベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて

、ベクトルv_i^2を求める行列作用部であって、前記非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、予め定められた、複数種類の演算子を組み合わせた演算方法に置換して、非可換行列Ａ１、Ａ２を作用させる行列作用部と、

前記行列作用部によって求められたベクトルv_i^1に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ１に結合させて前記ビット列Ｗ１を求めると共に、ベクトルv_i^2に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ２に結合させて前記ビット列Ｗ２を求めるビット列変換部と、

前記ビット列変換部によって求められた前記ビット列Ｗ１及び前記ビット列Ｗ２の各々のビット数が、暗号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すビット数判定部と、

前記ビット列Ｗ１及び前記ビット列Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求める擬似乱数列発生部と、

前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記暗号化対象データを表わすビット列との排他的論理和を計算することにより、前記暗号化対象データを暗号化する暗号化部と、

を含む暗号化装置。

［請求項4］ 暗号化装置と共通に設定された、請求項１又は２の共有秘密鍵生成装置によって生成された共有秘密鍵M_{AB}、及び２つの素数ｐ１、ｐ２に基づいて、２つの非可換行列Ａ１、Ａ２を生成する行列生成部と、

前記暗号化装置と共通に設定されたｄ次元の初期ベクトルv_0又は前回求められたｄ次元のベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1を求めると共に、前記初期ベクトルv_0、又は前回求められたｄ次元のベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、ベクトルv_i^2を求める行列作用部であって、前記非可換行列Ａ１、

Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、予め定められた、複数種類の演算子を組み合わせた演算方法に置換して、非可換行列Ａ１、Ａ２を作用させる行列作用部と、

前記行列作用部によって求められたベクトルv_i^1に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ１に結合させて前記ビット列Ｗ１を求めると共に、ベクトルv_i^2に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ２に結合させて前記ビット列Ｗ２を求めるビット列変換部と、

前記ビット列変換部によって求められた前記ビット列Ｗ１及び前記ビット列Ｗ２の各々のビット数が、復号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すビット数判定部と、

前記ビット列Ｗ１及び前記ビット列Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求める擬似乱数列発生部と、

前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記復号化対象データを表わすビット列との排他的論理和を計算することにより、前記復号化対象データを復号化する復号化部と、

を含む復号化装置。

［請求項5］ コンピュータを、

素数ｐ、自然数ｄ、行列式の値が１ではないｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を含む公開データを設定する公開データ設定部、

自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成する秘密鍵生成部、

前記秘密鍵を用いて、以下の（ＩＶ）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信相手へ送信する行列計算部、

前記通信相手の秘密鍵に含まれる自然数n_B（ｍｏｄ　ｐ）、k_B（

ｍｏｄ　ｐ）を用いて以下の（Ｖ）式に従って計算される、ｄ×ｄの行列M_B（ｍｏｄ　ｐ）を取得する行列取得部、及び

前記行列取得部によって取得された行列M_Bを用いて、以下の（ＶＩ）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を共有秘密鍵として算出する共有秘密鍵算出部

として機能させるためのプログラム。

$M_A = S^{-kA} Q^{nA} S^{kA}$　　・・・（ＩＶ）

$M_B = S^{-kB} Q^{nB} S^{kB}$　　・・・（Ｖ）

$M_{AB} = S^{-kA} M_B^{nA} S^{kA}$　　・・・（ＶＩ）

［請求項6］　公開データ設定部によって、素数ｐ、自然数ｄ、行列式の値が１ではないｄ×ｄの行列Ｑ（ｍｏｄ　ｐ）、及び逆行列が存在するｄ×ｄの行列Ｓ（ｍｏｄ　ｐ）を含む公開データを設定するステップと、

秘密鍵生成部によって、自然数n_A（ｍｏｄ　ｐ）、k_A（ｍｏｄ　ｐ）を含む秘密鍵を生成するステップと、

行列計算部によって、前記秘密鍵を用いて、以下の（ＶＩＩ）式に従って、ｄ×ｄの行列M_A（ｍｏｄ　ｐ）を計算し、通信相手へ送信するステップと、

行列取得部によって、前記通信相手の秘密鍵に含まれる自然数n_B（ｍｏｄ　ｐ）、k_B（ｍｏｄ　ｐ）を用いて以下の（ＶＩＩＩ）式に従って計算される、ｄ×ｄの行列M_B（ｍｏｄ　ｐ）を取得するステップと、

共有秘密鍵算出部によって、前記行列取得部によって取得された行列M_Bを用いて、以下の（ＩＸ）式に従ってｄ×ｄの行列M_{AB}（ｍｏｄ　ｐ）を共有秘密鍵として算出するステップと、

を含む共有秘密鍵生成方法。

$M_A = S^{-kA} Q^{nA} S^{kA}$　　・・・（ＶＩＩ）

$M_B = S^{-kB} Q^{nB} S^{kB}$　　・・・（ＶＩＩＩ）

$M_{AB} = S^{-kA} M_B^{nA} S^{kA}$　　・・・（ＩＸ）

［請求項7］ 行列生成部によって、復号化装置と共通に設定された、請求項６の共有秘密鍵生成方法によって生成された共有秘密鍵M_{AB}、及び２つの素数ｐ１、ｐ２に基づいて、２つの非可換行列Ａ１、Ａ２を生成するステップと、

行列作用部によって、前記復号化装置と共通に設定されたｄ次元の初期ベクトルv_0又は前回求められたｄ次元のベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1を求めると共に、前記初期ベクトルv_0、又は前回求められたｄ次元のベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、ベクトルv_i^2を求める行列作用部であって、前記非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、予め定められた、複数種類の演算子を組み合わせた演算方法に置換して、非可換行列Ａ１、Ａ２を作用させるステップと、

ビット列変換部によって、前記行列作用部によって求められたベクトルv_i^1に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ１に結合させて前記ビット列Ｗ１を求めると共に、ベクトルv_i^2に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ２に結合させて前記ビット列Ｗ２を求めるステップと、

ビット数判定部によって、前記ビット列変換部によって求められた前記ビット列Ｗ１及び前記ビット列Ｗ２の各々のビット数が、暗号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すステップと、

擬似乱数列発生部によって、前記ビット列Ｗ１及び前記ビット列Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求めるステップと、

暗号化部によって、前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記暗号化対象データを表わすビット列との排他的

論理和を計算することにより、前記暗号化対象データを暗号化するステップと、

を含む暗号化方法。

［請求項8］ 行列生成部によって、暗号化装置と共通に設定された、請求項１又は２の共有秘密鍵生成方法によって生成された共有秘密鍵M_{AB}、及び２つの素数ｐ１、ｐ２に基づいて、２つの非可換行列Ａ１、Ａ２を生成するステップと、

行列作用部によって、前記暗号化装置と共通に設定されたｄ次元の初期ベクトルv_0又は前回求められたｄ次元のベクトルv_{i-1}^1に、非可換行列Ａ１を作用させて、ベクトルv_i^1を求めると共に、前記初期ベクトルv_0、又は前回求められたｄ次元のベクトルv_{i-1}^2に、非可換行列Ａ２を作用させて、ベクトルv_i^2を求める行列作用部であって、前記非可換行列Ａ１、Ａ２を作用させる際の和演算及び積演算の少なくとも一方を、予め定められた、複数種類の演算子を組み合わせた演算方法に置換して、非可換行列Ａ１、Ａ２を作用させるステップと、

ビット列変換部によって、前記行列作用部によって求められたベクトルv_i^1に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ１に結合させて前記ビット列Ｗ１を求めると共に、ベクトルv_i^2に対して非線形変換を行ってビット列に変換し、前記変換したビット列を前回求められたビット列Ｗ２に結合させて前記ビット列Ｗ２を求めるステップと、

ビット数判定部によって、前記ビット列変換部によって求められた前記ビット列Ｗ１及び前記ビット列Ｗ２の各々のビット数が、復号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すステップと、

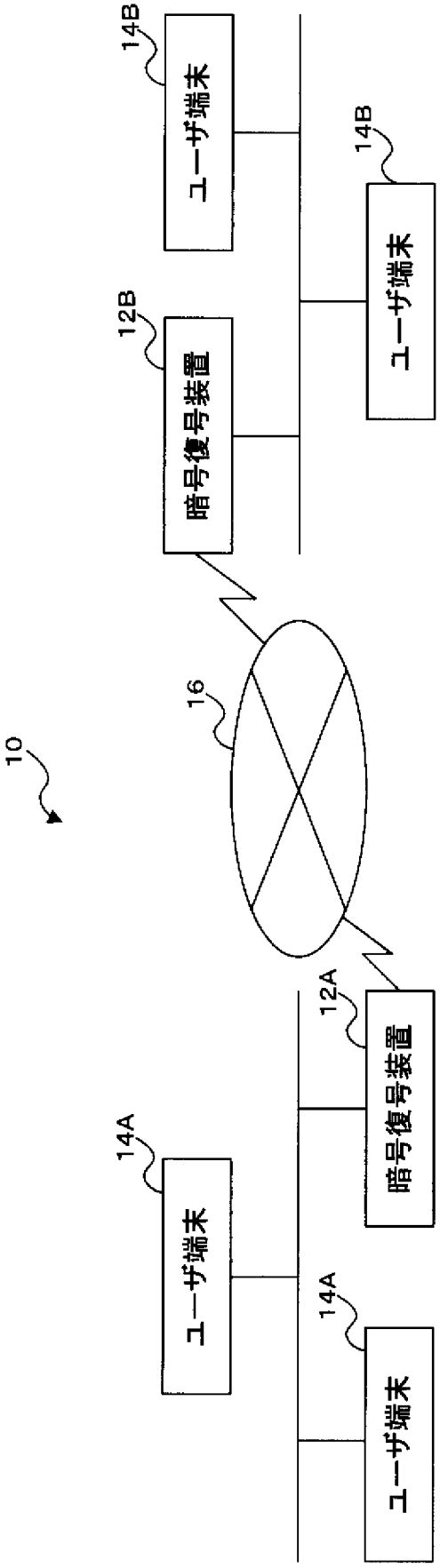
擬似乱数列発生部によって、前記ビット列Ｗ１及び前記ビット列Ｗ２の排他的論理和を計算して、擬似乱数ビット列を求めるステップと

、

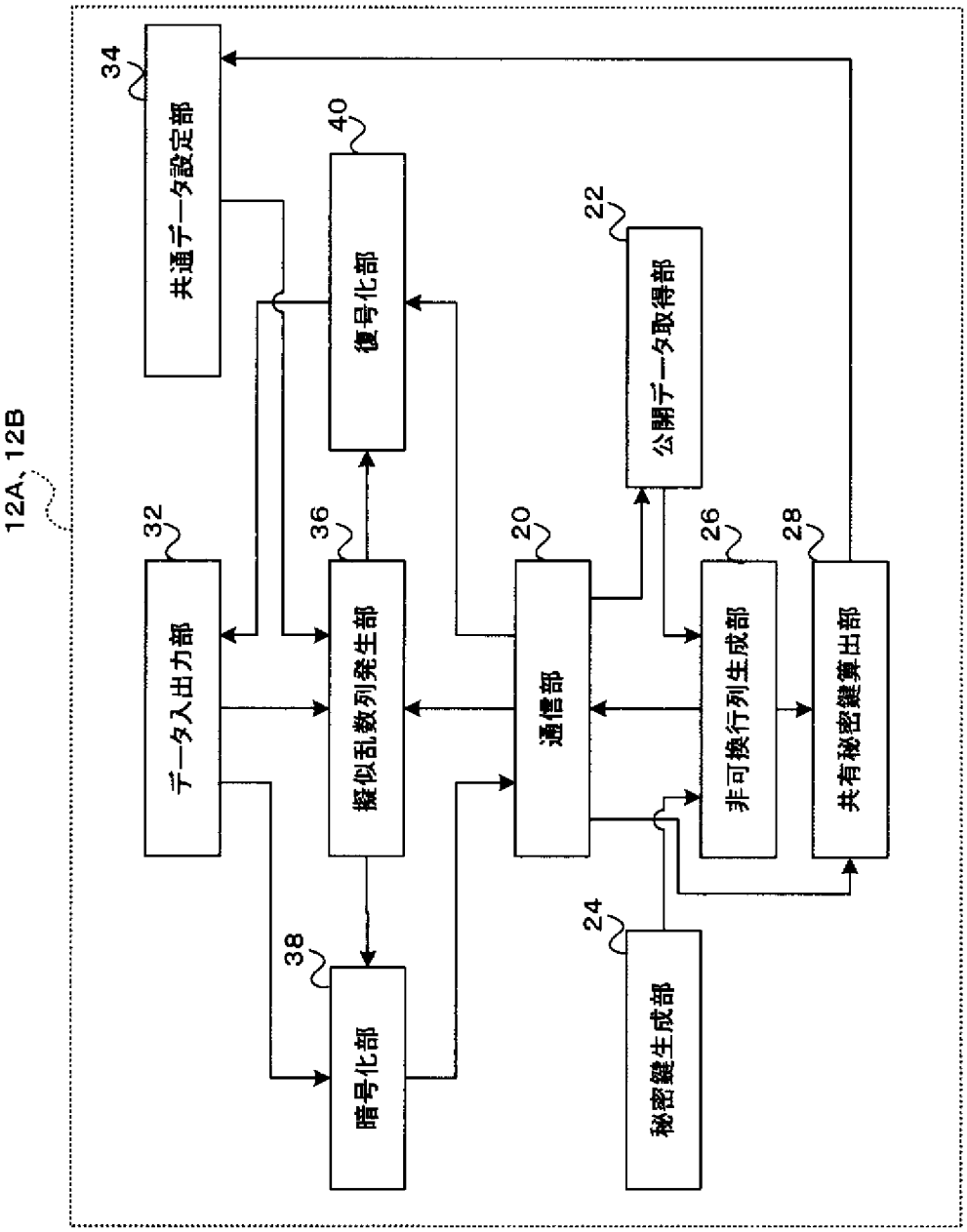
復号化部によって、前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記復号化対象データを表わすビット列との排他的論理和を計算することにより、前記復号化対象データを復号化するステップと、

を含む復号化方法。

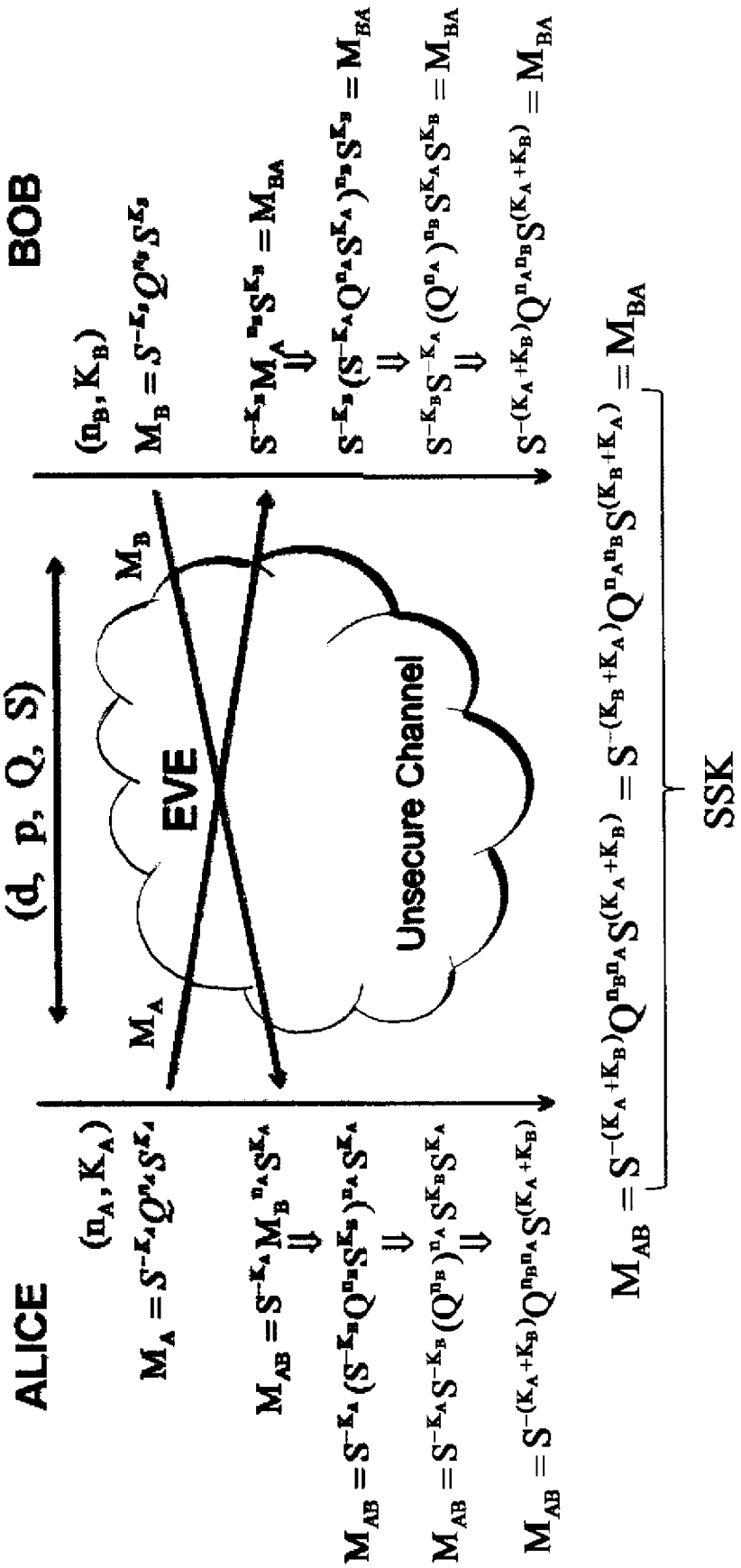
[図1]


10
16
12A
暗号復号装置
12B
暗号復号装置
14A
ユーザ端末
14A
ユーザ端末
14B
ユーザ端末
14B
ユーザ端末

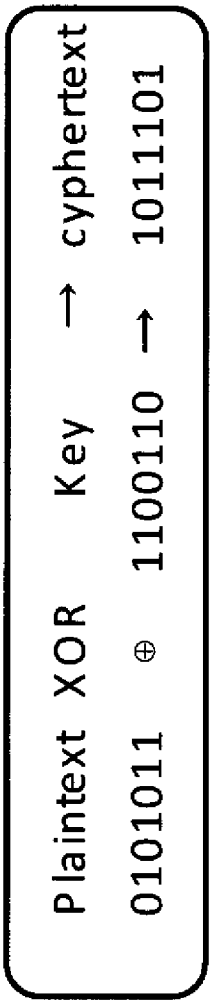
[図2]


12A、12B
34
共通データ設定部
40
復号化部
22
公開データ取得部
32
データ入出力部
36
擬似乱数列発生部
20
通信部
26
非可換行列生成部
28
共有秘密鍵算出部
38
暗号化部
24
秘密鍵生成部

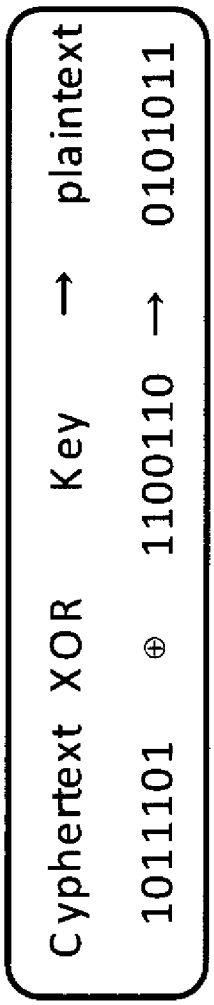
[図3]


ALICE
BOB
(d, p, Q, S)
EVE
Unsecure Channel
(n_A, K_A)
$M_A = S^{-K_A} Q^{n_A} S^{K_A}$
$M_{AB} = S^{-K_A} M_B^{\ n_A} S^{K_A}$
$M_{AB} = S^{-K_A} (S^{-K_B} Q^{n_B} S^{K_B})^{n_A} S^{K_A}$
$M_{AB} = S^{-K_A} S^{-K_B} (Q^{n_B})^{n_A} S^{K_B} S^{K_A}$
$M_{AB} = S^{-(K_A+K_B)} Q^{n_B n_A} S^{(K_A+K_B)}$
(n_B, K_B)
$M_B = S^{-K_B} Q^{n_B} S^{K_B}$
$S^{-K_B} M_A^{\ n_B} S^{K_B} = M_{BA}$
$S^{-K_B} (S^{-K_A} Q^{n_A} S^{K_A})^{n_B} S^{K_B} = M_{BA}$
$S^{-K_B} S^{-K_A} (Q^{n_A})^{n_B} S^{K_A} S^{K_B} = M_{BA}$
$S^{-(K_A+K_B)} Q^{n_A n_B} S^{(K_A+K_B)} = M_{BA}$
$M_{AB} = S^{-(K_A+K_B)} Q^{n_B n_A} S^{(K_A+K_B)} = S^{-(K_B+K_A)} Q^{n_A n_B} S^{(K_B+K_A)} = M_{BA}$
SSK

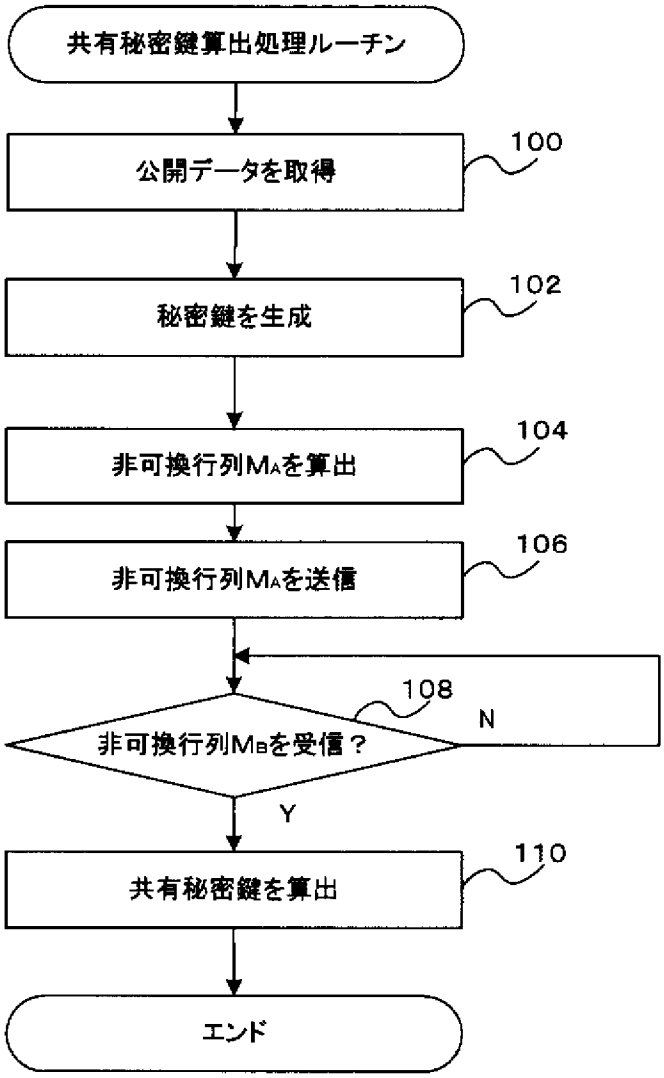
[図4A]


Plaintext XOR Key → cyphertext
0101011 ⊕ 1100110 → 10111101
暗号化

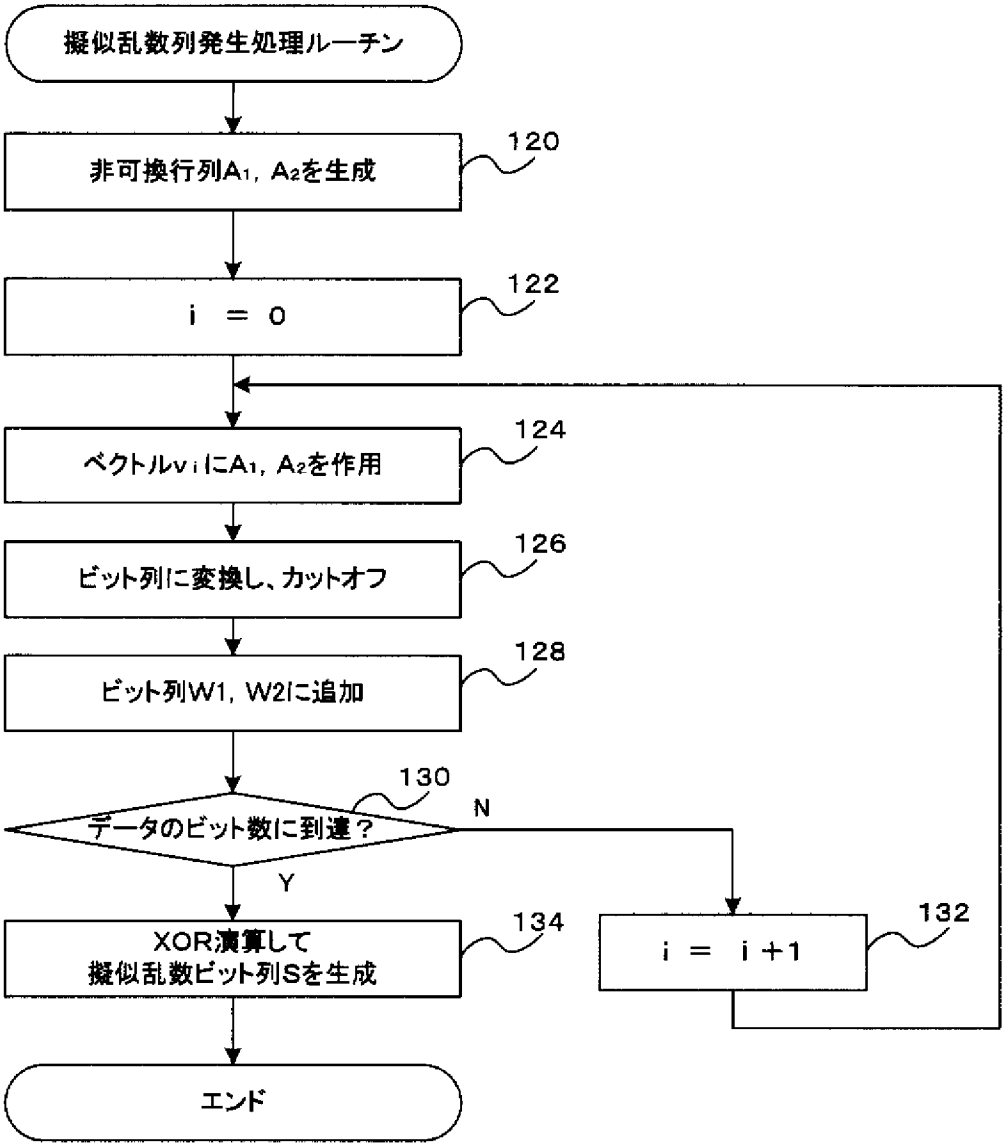
[図4B]


Cyphertext XOR Key → plaintext
10111101 ⊕ 1100110 → 0101011
復号化

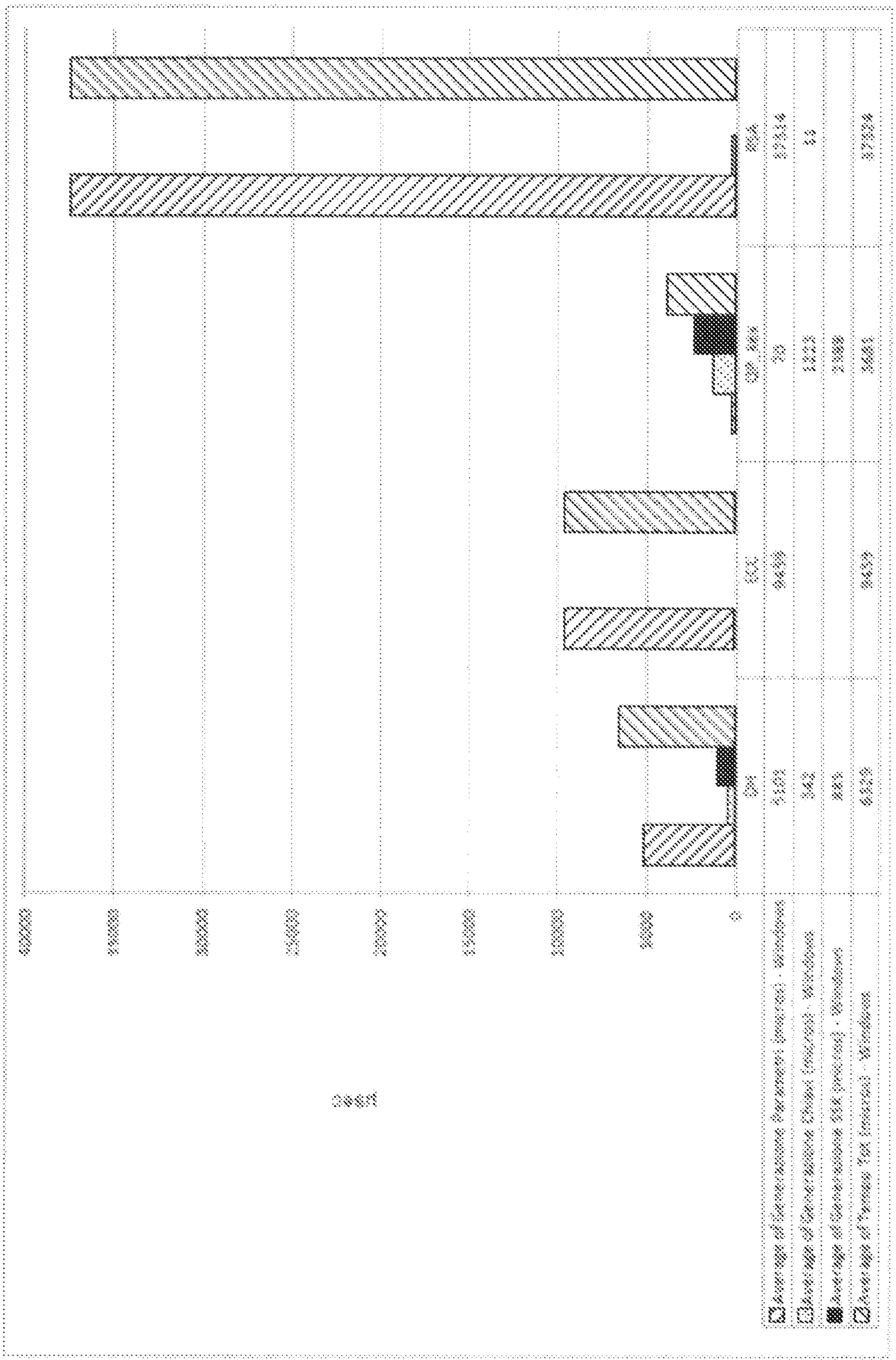
[図5]


共有秘密鍵算出処理ルーチン
公開データを取得
100
秘密鍵を生成
102
非可換行列MAを算出
104
非可換行列MAを送信
106
非可換行列MBを受信？
108
N
Y
共有秘密鍵を算出
110
エンド

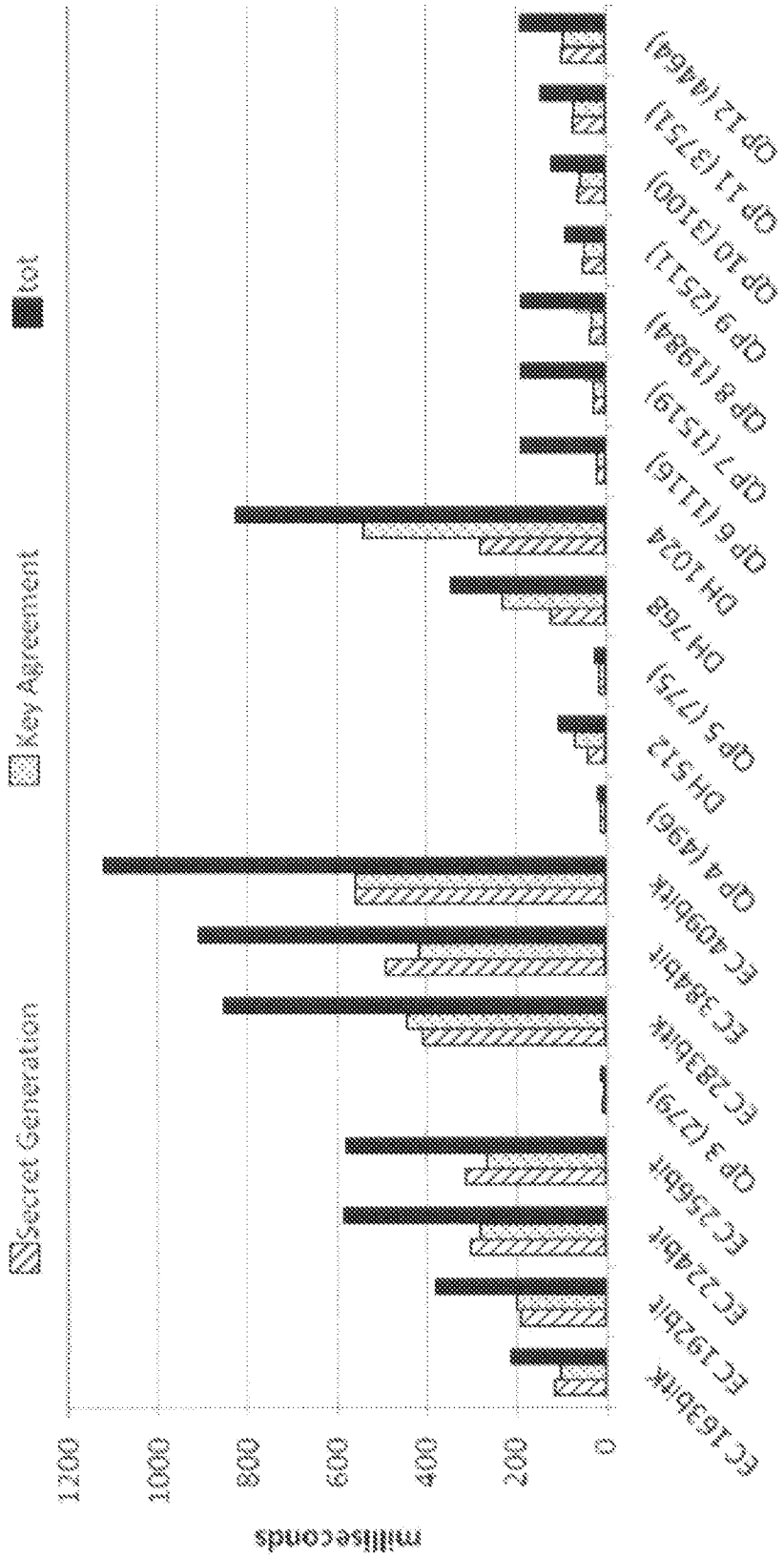
[図6]


擬似乱数列発生処理ルーチン
非可換行列A1, A2を生成
120
i = 0
122
ベクトルvi にA1, A2を作用
124
ビット列に変換し、カットオフ
126
ビット列W1, W2に追加
128
データのビット数に到達？
130
N
Y
XOR演算して
擬似乱数ビット列Sを生成
134
i = i +1
132
エンド

[図7]



[図8]


Secret Generation
Key Agreement
Total
milliseconds
0
200
400
600
800
1000
1200
EC 163bit
EC 192bit
EC 224bit
EC 256bit
DP 3 (279)
EC 283bit
EC 384bit
EC 409bit
DP 4 (496)
DH 512
DP 5 (779)
DH 768
DH 1024
DP 6 (1116)
DP 7 (1519)
DP 8 (1984)
DP 9 (2511)
DP 10 (3100)
DP 11 (3753)
DP 12 (4464)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068419

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *H04L9/20*(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, H04L9/20

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 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IEEE Xplore, CiNii, THE ACM DIGITAL LIBRARY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Ottaviani, V. et al, Conjugation as public key agreement protocol in mobile cryptography, Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference, 2010.07, p.1-6	1,2,5,6 3,4,7,8
Y	JP 7-212356 A (International Business Machines Corp.), 11 August 1995 (11.08.1995), paragraph [0021]; fig. 3 & US 5491749 A & EP 661844 A2	1,2,5,6
Y	JP 2007-288254 A (Sony Corp.), 01 November 2007 (01.11.2007), paragraphs [0044] to [0102]; fig. 3, 4 & US 2007/0242822 A1 & EP 1845653 A1	2

☒ 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
25 July, 2013 (25.07.13)	06 August, 2013 (06.08.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068419

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Accardi, L et al, The QP-DYN algorithms, [online], 2011, [retrieved on 08 April 2013 (08.04.2013)], Internet <URL:http://www.cryptalarm.it/ca/documenti/upload2set/8125_chap01.pdf>	3,4,7,8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０６８４１９

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, H04L9/20(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, H04L9/20

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	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３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）

IEEE Xplore, CiNii, THE ACM DIGITAL LIBRARY

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	Ottaviani, V. et al, Conjugation as public key agreement protocol in mobile cryptography, Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference, 2010.07, p.1-6	１，２，５，６
A		３，４，７，８
Y	JP 7-212356 A（インターナショナル・ビジネス・マシーンズ・コーポレイション）1995.08.11, 段落【００２１】,【図３】 & US 5491749 A & EP 661844 A2	１，２，５，６

☑　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
２５．０７．２０１３	０６．０８．２０１３

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　３１４６
松平　英
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 2007-288254 A（ソニー株式会社）2007.11.01，段落【００４４】－【０１０２】，【図３】，【図４】 & US 2007/0242822 A1 & EP 1845653 A1	２
Ａ	Accardi, L et al, The QP-DYN algorithms, [online], 2011, [平成２５年４月８日検索], インターネット <URL:http://www.cryptalarm.it/ca/documenti/upload2set/8125_chap01.pdf>	３，４，７，８