

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2013 年 10 月 10 日(10.10.2013)



(10) 国際公開番号

WO 2013/150880 A1

- (51) 国際特許分類:
H04L 9/20 (2006.01)
- (21) 国際出願番号: PCT/JP2013/057509
- (22) 国際出願日: 2013 年 3 月 15 日(15.03.2013)
- (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 2012-084113 2012 年 4 月 2 日(02.04.2012) JP
- (71) 出願人: 学校法人東京理科大学(TOKYO UNIVERSITY OF SCIENCE FOUNDATION) [JP/JP]; 〒1628601 東京都新宿区神楽坂一丁目 3 番地 Tokyo (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 テペリオ 1 8、ローマ
Rome (IT). レゴリ マッシモ(REGOLI, Massimo);
00044 ヴィア フォンターナ ヴェッチャ 1
8、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 1 7 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, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS,
LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, 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.

[続葉有]

(54) Title: ENCRYPTION DEVICE, DECRYPTION DEVICE, ENCRYPTION METHOD, DECRYPTION METHOD, AND PROGRAM

(54) 発明の名称: 暗号化装置、復号化装置、暗号化方法、復号化方法、及びプログラム

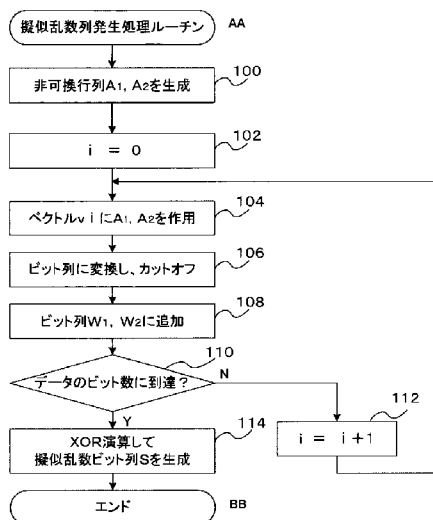


FIG. 4:
AA Pseudorandom number string generation
process routine
100 Generate noncommutative matrices (A_1, A_2)
104 Apply vector (V) to A_1, A_2
106 Convert to bit string, cut off
108 Add to bit strings (W_1, W_2)
110 Data bit number reached?
114 Compute XOR, generate pseudorandom
number bit string (S)
BB End

(57) Abstract: On the basis of private data (A) and prime numbers (p_1, p_2), an encryption device generates noncommutative matrices (A_1, A_2) (100) and applies the noncommutative matrices (A_1, A_2) to vectors (v_{i-1}^1, v_{i-1}^2) (104). The encryption device carries out a nonlinear conversion on the vector (v_{i-1}^1) and the vector (v_{i-1}^2), converting same to bit strings, and bonds same with bit strings (W_1, W_2) (106, 108). The encryption device repeats the application of the noncommutative matrices and the nonlinear conversion until the number of bits of the bit string (W_1) and the bit string (W_2) reach a number of bits of a bit string which represents data to be encrypted (110). The encryption device calculates an exclusive OR (XOR) of the bit string (W_1) and the bit string (W_2), derives a pseudorandom bit string (112), and carries out encryption using the pseudorandom bit string. Thus, it is possible for the encryption device to accelerate an encryption process and strengthen encryption breaking resist-
ance when a number of bits of data to be encrypted is variable.

(57) 要約: 暗号化装置は、プライベートデータ A 及び素数 p_1, p_2 に基づいて、非可換行列 A_1, A_2 を生成し (100)、ベクトル v_{i-1}^1, v_{i-1}^2 に、非可換行列 A_1, A_2 を作用させる (104)。暗号化装置は、ベクトル v_{i-1}^1 、ベクトル v_{i-1}^2 に対して非線形変換を行ってビット列に変換し、ビット列 W_1, W_2 に結合させる (106, 108)。暗号化装置は、ビット列 W_1 及びビット列 W_2 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、非可換行列の作用及び非線形変換を繰り返す (110)。暗号化装置は、ビット列 W_1 及びビット列 W_2 の排他的論理和を計算して、擬似乱数ビット列を求め (112)、擬似乱数ビット列を用いて暗号化を行う。これにより、暗号化装置は、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。



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

暗号化装置、復号化装置、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、暗号化装置、復号化装置、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、暗号化処理を高速、かつ暗号解読強度を強くする暗号化装置が知られている（特開2003-241656号公報）。この暗号化装置では、初期処理関数により、平文Dを分割し複数の分割データとして出力し、複数の分割データを演算関数により暗号鍵Kと同じ大きさに拡大置換し、係数を媒介することにより演算関数を可変にする。その係数は、媒介変数生成部により生成される。そして、非線形暗号化ブロック処理部により、分割データと暗号鍵Kとを変数として非線形に暗号化し、暗号化した複数の分割暗号化データを出力する。さらに、後処理関数により、演算関数の逆関数を使い分割暗号化データを分割データと同じ大きさに縮小置換し、分割データを合成し暗号文として出力し、係数を媒介することにより逆関数の演算関数を可変にする。

[0003] また、秘密情報a、bと乱数情報m1、m2とを排他的論理和により加算することによって秘密情報a、bをマスクし、マスクされた秘密情報A、Bを算出する手段と、マスクされた秘密情報A、Bと乱数情報m1、m2とを用いて、マスクされた秘密情報A、Bのマスクを除去するための中間値Temp1～Temp3を算出する手段と、マスクされた秘密情報A、Bと中間値Temp1～Temp3を用いて、秘密情報a、bの論理積や論理和に関する演算を行う手段とを備えた暗号処理装置が知られている（特開2009-005164号公報）。

[0004] 特開2003-241656号公報、特開2009-005164号公報によって開示された暗号処理技術は暗号化処理の高速性、安全性の高度化を図るものであるが、理論

的に解読が可能であるという潜在的な危険性を有する等の問題を抱えている。この問題を解消するためには容量が大きくなって高速性を犠牲にされる場合があり、「高速」、「安全」、「軽量」という暗号化処理の要求を総合的に満足させる技術はなかった。そこで、理論上は解読不能な非可換関数を元にした暗号方式が提案されている (L. Accardi, M. Regoli, M. Ohya, “The QP-DYN Algorithm”, QP-PQ 28, Quantum Bio-Informatics IV, 1-16, 2011)。

発明の開示

発明が解決しようとする課題

[0005] L. Accardi, M. Regoli, M. Ohya, “The QP-DYN Algorithm”, QP-PQ 28, Quantum Bio-Informatics IV, 1-16, 2011によって開示された技術では暗号化処理の概念は示されているが、高速性と暗号の頑健性を決定する力学系への変換やベクトル列の導出などを設定すること、さらにはこの暗号化処理を装置に実装することは困難であった。

[0006] 本発明は、前記課題を鑑み、なされたものである。

課題を解決するための手段

[0007] 上記の目的を達成するために第1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、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 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 W_1 に

結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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。

[0008] 第2の態様に係るプログラムは、コンピュータを、復号化装置と共通に設定された、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 を生成する行列生成部、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} に、非可換行列 A_1 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} に、非可換行列 A_2 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 A_1 、 A_2 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 A_1 、 A_2 を作用させる行列作用部、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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 を求めるビット列変換部、前記ビット列変換部によって求められた前記ビット列 W_1 及び前記ビット列 W_2 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、前記ビット列 W_1 及び前記ビット列 W_2 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、及び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して機能させるためのプログラムである。

[0009] このように、非可換行列 A_1 、 A_2 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 A_1 、 A_2 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 W_1 、 W_2 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。

[0010] 第3の態様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 A_1 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 A_1 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 A_2 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 A_2 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。

[0011] 第4の態様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 W_1 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 W_2 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。

[0012] また、第5の態様に係るビット列変換部は、前記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。

[0013] 第6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、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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W 1 及び前記ビット列W 2 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。

[0014] 第7の態様に係るプログラムは、コンピュータを、暗号化装置と共通に設定された、プライベートデータである $d \times d$ の行列A、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列A 1、A 2を生成する行列生成部、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A 1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A 2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A 1、A 2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A 1、A 2を作用させる行列作用部、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W 1に結合させて前記ビット列W 1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W 2に結合させて前記ビット列W 2を求めるビット列変換部、前記ビット列変換部によって求められた前記ビット列W 1及び前記ビット列W 2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、前記ビット列W 1及び前記ビット列W 2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、及び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して機能させるためのプログラムである。

[0015] このように、非可換行列 A_1 、 A_2 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 A_1 、 A_2 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 W_1 、 W_2 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復号化することにより、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、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。

発明の効果

[0016] 本発明の一態様である暗号化装置、復号化装置、暗号化方法、復号化方法、及びプログラムによれば、非可換行列 A_1 、 A_2 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 A_1 、 A_2 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 W_1 、 W_2 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

[0017] [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3A]暗号化方法を説明するための図である。

[図3B]復号化方法を説明するための図である。

[図4]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5]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

[0018] 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。

[0019] <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。

[0020] 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。

[0021] 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、一方、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。

[0022] 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、一方、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。

[0023] 暗号復号装置12A、12Bは、CPU (Central Processing Unit) と、RAM (Random Access Memory) と、後述する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、データ入出力部2

2、共通データ設定部24、擬似乱数列発生部26、暗号化部28、及び復号化部30を備えている。なお、擬似乱数列発生部26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。

[0024] 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。

[0025] データ入出力部22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。

[0026] 共通データ設定部24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、プライベートデータである $d \times d$ の行列A、素数 p_1 、 p_2 、初期ベクトル v_0 が共通のデータとして設定される。

[0027] 擬似乱数列発生部26は、後述する手法により、プライベートデータである $d \times d$ の行列A、素数 p_1 、 p_2 、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。

[0028] 暗号化部28は、擬似乱数列発生部26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22により入力された暗号化対象データに対して、ストリーム暗号を行う。例えば、図3A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28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。

[0029] 復号化部30は、擬似乱数列発生部26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、図3B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30により復号化されたデータ

は、データ入出力部 22 により、データ端末 14 A、14 B へ出力される。

[0030] 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。

[0031] まず、擬似乱数列発生部 26 は、共通のプライベートデータとして設定された $d \times d$ の行列 A 及び素数 p_1 、 p_2 とを用いて、以下のように、2 つの非可換行列 A_1 、 A_2 を生成する。なお、以下では、行列 A が、 2×2 の行列である場合を例に説明する。

[0032] 擬似乱数列発生部 26 は、以下の (1) 式に示すように、行列 A と素数 p_1 とを用いて、行列 A_1' を計算する。

[0033] [数1]

$$\begin{aligned} A_1' &= A \bmod p_1 \\ &= \begin{pmatrix} a \bmod p_1 & b \bmod p_1 \\ c \bmod p_1 & d \bmod p_1 \end{pmatrix} \\ &= \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \end{aligned} \quad \dots (1)$$

[0034] そして、擬似乱数列発生部 26 は、 $\langle g \rangle = \{1, \dots, p_1 - 1\}$ 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、 $\langle 3 \rangle = \{1, \dots, 6\}$ である。

[0035] $3^1 = 3$, $3^2 = 9 \bmod 7 = 2$, $3^3 = 27 \bmod 7 = 6$, $3^4 = 81 \bmod 7 = 4$,
 $3^5 = 243 \bmod 7 = 5$, $\dots$

[0036] そして、擬似乱数列発生部 26 は、 A_1'' を、以下の (2) 式で表わすとすると、 $\det A_1'' = g$ 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 A_1 とする。

[0037] [数2]

$$A_1'' = \begin{pmatrix} g & b' \\ c' & d' \end{pmatrix}, \quad \dots \quad (2)$$

[0038] また、擬似乱数列発生部26は、以下の(3)式に示すように、行列Aと素数 p_2 とを用いて、行列 A_2' を計算し、上記と同様に、非可換行列 A_2 を生成する。

[0039] [数3]

$$\begin{aligned} A_2' &= A \bmod p_2 \\ &= \begin{pmatrix} a \bmod p_2 & b \bmod p_2 \\ c \bmod p_2 & d \bmod p_2 \end{pmatrix} \quad \dots \quad (3) \end{aligned}$$

[0040] ここで、非可換行列 A_1 、 A_2 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 A_1 、 A_2 の生成に用いる、任意の素数 p を用いて、以下の(4)式のように書ける。

[0041] $O(A) \geq p \quad \dots \quad (4)$

[0042] たとえば、 p を100000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。

[0043] また、擬似乱数列発生部26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、擬似乱数列発生部26は、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 $V = \{v_0, v_1, \dots, v_t\}$ を得る。ここで $v_i = A_1^i v_0$ である。

[0044] そして、擬似乱数列発生部26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 W_1 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 $v_i = (v_{i,0}, v_{i,1}, \dots, v_{i,n})$ 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。

[0045] 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。

[0046] 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。

[0047] 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。

[0048] 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 A_1 と A_2 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。

[0049] また、本実施の形態では、ベクトル v_i に、非可換行列 A_1 、 A_2 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。

[0050] 例えば、a、bを32bitの数とし、記号 $a \ll k$ を、aをkビットずらす記号とすると、(和演算) $a+b$ を、 $a+b \bmod 2^{32}$ に置き換える。また、(積演算) $a \times b$ を、 $a \ll (b / 2^{27}) \text{ xor } b$ に置き換える。ここで、 $a \ll (b / 2^{27})$ 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。

[0051] また、ベクトル v_i に、非可換行列 A_1 、 A_2 を作用させて、新しいベクトル

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。

[0052] 例えば、 $v_i = (v_i^1, v_i^2, \dots, v_i^d)$ 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、 $v_{i+1} = (v_{i+1}^1, v_{i+1}^2, \dots, v_{i+1}^d)$ を得る方法を以下のようにする。

[0053] まず、 $v_{i+1}^1 = (A v_i)^1$ とする。これはベクトル $A v_i$ 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、

[0054] [数4]

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

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。

[0055] そして、 $v_{i+1}^2 = (A (v_{i+1}^1, v_i^2, \dots, v_i^d))^2$ 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。

[0056] そして、 $v_{i+1}^3 = (A (v_{i+1}^1, v_{i+1}^2, \dots, v_i^d))^3$ 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。

[0057] 以降、 d 番目の要素まで同様に行い、 v_{i+1} を得る。

[0058] 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。

[0059] 擬似乱数列発生部 26 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 W_2 を生成する。また、ビット列 W_2 のビット数が n に到達した瞬間、ビット列 W_2 に対する処理は中断され、ビット列 W_2 の余った部分は捨てられる。

[0060] そして、擬似乱数列発生部 26 は、最終的に得られたビット列 W_1 とビット列 W_2 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 W_1 とビット列 W_2 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。

[0061] 擬似乱数列発生部 26 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。

[0062] <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。

[0063] まず、ユーザ端末 14 A から、データをユーザ端末 14 B へ送信する場合に、ユーザ端末 14 A が、送信データを、暗号復号装置 12 A に出力する。

[0064] また、暗号復号装置 12 A において、図 4 に示す擬似乱数列発生処理ルーチンが実行される。

[0065] まず、ステップ 100 において、暗号復号装置 12 A は、暗号復号装置 12 B と共通に設定された非可換行列 A 、素数 p_1 、 p_2 を用いて、非可換行列 A_1 、 A_2 を生成する。ステップ 102 では、暗号復号装置 12 A 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、初期ベクトル v_0 を設定する。

[0066] 次のステップ 104 では、暗号復号装置 12 A は、ベクトル v_i に、非可換行列 A_1 、 A_2 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 106 では、上記ステップ 104 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108において、暗号復号装置12Aは、上記ステップ106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。

[0067] ステップ110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112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104へ戻って、ステップ104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104以降の処理において、暗号復号装置12Aは、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104以降の処理において、暗号復号装置12Aは、非可換行列A2を用いた処理は行わない。

[0068] また、上記ステップ110において、暗号復号装置12Aは、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114へ進む。

[0069] ステップ114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。

[0070] 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。

[0071] 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 4 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。

[0072] 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。

[0073] 前記した実施形態の一構成要素にあたる擬似乱数列は本発明を創作する過程で統計テスト (NISTU01 テスト) を実施している (F. Giuseppe, “Benchmarking for the QP Cryptographic Suite”, Dipartimento di Informatica, Sistemi e Produzione, Università di Roma “Tor Vergata” (イタリア語)、2009 参照)。以下、NISTU01 テストの結果について簡単に説明するが、本テストは、プログラムソースがクローズされた状態で入出力の状態のみを取得して行っているものである。ここで、NIST とは米国立標準技術研究所であって、NISTU01 テストは、NIST が米国の政府機関での使用を認める暗号アルゴリズムおよび実装の要件を課す目的で実施しているテストの一つであり、疑似乱数列の安全性を評価するものである。

[0074] U01 は C ライブラリで提供されているものを用いた。テストには、SmallCrush, BigCrash, Rabbit, Alphabit, FIPS-140-2, pseudoDIEHARD が含まれている。ここで、現在広く用いられている擬似乱数列発生アルゴリズム RC4 を比較対象とした。

[0075] 前記した実施形態の一構成要素にあたる擬似乱数列は、全ての統計テストをパスしたが、比較対象である RC4 は、多くのテストをパスできなかった。これにより、実施の形態で説明した擬似乱数列の発生アルゴリズムでは、

統計的に安全な擬似乱数列を生成できることが分かった。

[0076] 続いて、前記した実施形態の一構成要素にあたる暗号化方法（以下、Q P
ー D Y Nとも称する。）についても本発明を創作する過程で実施した実験結
果について説明する。

[0077] この実験は、暗号化速度を検証することを目的に、ストリーム暗号の暗号
化速度の検証を実施している（P e r f o r m a n c e A n a l y s i s
o f A l g o r i t h m s a n d S t a t i s t i c a l T e s
t s,（イタリア語），2011）。なお、この実験についても、前記した
N I S T U 0 1テストと同様に、プログラムソースがクローズされた状態で
入出力の状態のみを取得して行っているものである。

[0078] 実験の環境は以下の通りである。W i n d o w s 7（登録商標）上のパフ
ォーマンスは、以下の表1に示す。

[0079] [表1]

CPU	E 5 3 0 0 @ 2 . 6 G H z I n t e l P e n t i u m
RAM	4 G B D D R 2 8 0 0 (v D a t a 2 x 2 G B)
HDD	5 0 0 G B 7 2 0 0 R P M (W e s t e r n D i g i t a l C a v i a r B l u e)
OS	M S W i n d o w s 7 3 2 - b i t

[0080] いくつかのファイル（10MB、100MB、p d fファイル、ディスク
イメージ（u b u n t u - 1 0 . 1 0 - d e s k t o p - i 3 8 6 . i s o
），m p 4ビデオ3.5G, W o r dドキュメント等）でデータの暗号化の
実験を行い、読み書きのプロセスまで含めた1秒あたりの暗号化データ量の
計測を行った。

[0081] 比較対象として、A E SとT w o F i s hを用いた。仕様を以下の表2に
示す。

[0082]

[表2]

QP-DYN	Key Size :	288 b and 1156 b
	Buffer size :	10,000 b
	Encryption modes :	OFB
AES	Key Size :	256 b
	Buffer size :	decided by the library cryptopp
	Encryption modes :	OFB
Twofishi	Key Size :	256 b
	Buffer size :	decided by the library cryptopp
	Encryption modes :	OFB

[0083] 各テストデータに対して暗号化における1秒あたりの暗号化データ量を計測し、平均を求めると、図5に示す実験結果が得られた。これより、256ビットの鍵長のAESとTwofishより、QP-DYN288ビットと1156ビットのほうが、1秒あたりの暗号化データ量が多いことが分かった。

[0084] 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、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。

[0085] 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。

[0086] 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。

[0087] 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。

[0088] 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。

[0089] 例えば、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。

[0090] 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。

[0091] 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、復号化装置と共通に設定された、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 を生成する行列生成部、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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 を作用させる行列作用部、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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 を求めるビット列変換部、前記ビット列変換部によって求められた前記ビット列 W_1 及び前記ビット列 W_2 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、前記ビット列 W_1 及び前記ビット列 W_2 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、及び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。

[0092] 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、暗号化装置と共通に設定された、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 を生成する行列生成部、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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 を作用させる行列作用部、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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 を求めるビット列変換部、前記ビット列変換部によって求められた前記ビット列 W_1 及び前記ビット列 W_2 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、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、及び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。

[0093] 日本出願2012-084113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。

[0094] 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]

復号化装置と共通に設定された、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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2] 前記行列作用部は、

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 A_1 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 A_1 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 A_2 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 A_2 を作用させて、ベクトル v_i^2 の前記要素を計算する請求項 1 記載の暗号化装置。

[請求項3] 前記ビット列変換部は、

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 W_1 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 W_2 に結合させる請求項 1 又は 2 記載の暗号化装置。

[請求項4] 前記ビット列変換部は、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請求項 3 記載の暗号化装置。

[請求項5] 暗号化装置と共通に設定された、プライベートデータである $d \times d$

の行列 A 、及び 2 つの素数 p_1 、 p_2 に基づいて、2 つの非可換行列 A_1 、 A_2 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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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6]

コンピュータを、

復号化装置と共通に設定された、プライベートデータである $d \times d$

の行列 A 、及び 2 つの素数 p_1 、 p_2 に基づいて、2 つの非可換行列 A_1 、 A_2 を生成する行列生成部、

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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 を作用させる行列作用部、

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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 を求めるビット列変換部、

前記ビット列変換部によって求められた前記ビット列 W_1 及び前記ビット列 W_2 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、

前記ビット列 W_1 及び前記ビット列 W_2 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、及び

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

として機能させるためのプログラム。

[請求項7]

コンピュータを、

暗号化装置と共通に設定された、プライベートデータである $d \times d$

の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 を生成する行列生成部、

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 A_1 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 A_2 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 A_1 、 A_2 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 A_1 、 A_2 を作用させる行列作用部、

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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 を求めるビット列変換部、

前記ビット列変換部によって求められた前記ビット列 W_1 及び前記ビット列 W_2 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、

前記ビット列 W_1 及び前記ビット列 W_2 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、及び

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

として機能させるためのプログラム。

[請求項8]

行列生成部によって、復号化装置と共通に設定された、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づい

て、2つの非可換行列 A_1 、 A_2 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 A_1 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 A_2 を作用させて、ベクトル v_i^2 を求めるステップであって、前記非可換行列 A_1 、 A_2 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 A_1 、 A_2 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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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 W_1 及び前記ビット列 W_2 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9] 行列生成部によって、暗号化装置と共通に設定された、プライベートデータである $d \times d$ の行列 A 、及び2つの素数 p_1 、 p_2 に基づいて、2つの非可換行列 A_1 、 A_2 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 A_1 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 A_2 を作用させて、ベクトル v_i^2 を求めるステップであって、前記非可換行列 A_1 、 A_2 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法に置換して、非可換行列 A_1 、 A_2 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 W_1 に結合させて前記ビット列 W_1 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 W_2 に結合させて前記ビット列 W_2 を求めるステップと、

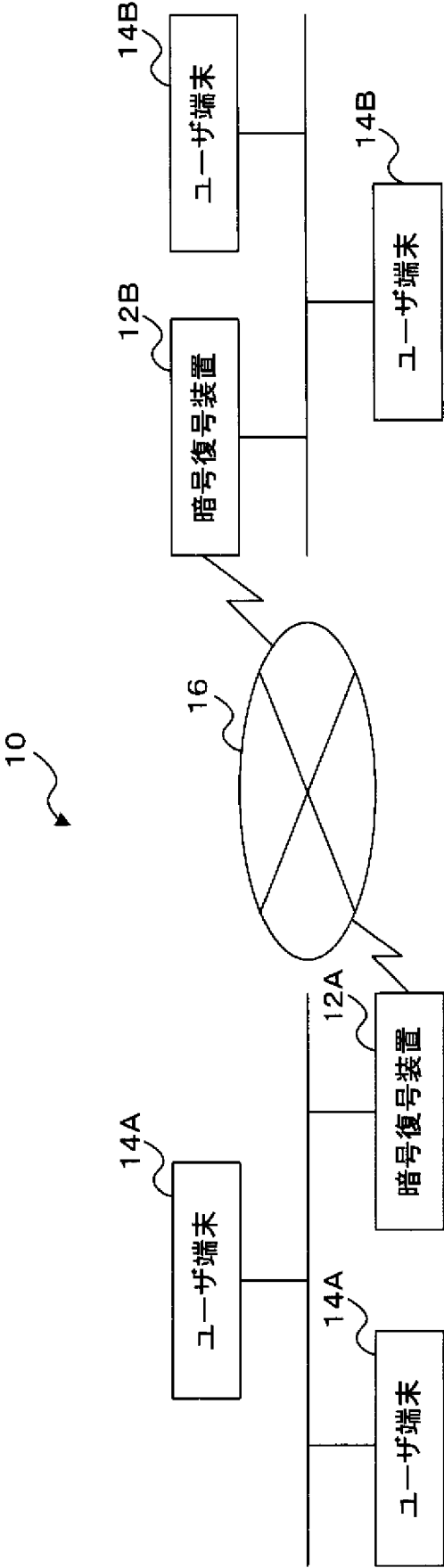
ビット数判定部によって、前記ビット列変換部によって求められた前記ビット列 W_1 及び前記ビット列 W_2 の各々のビット数が、復号化対象データを表わすビット列のビット数になるまで、前記行列作用部による作用と前記ビット列変換部による変換及び結合とを繰り返すステップと、

擬似乱数列発生部によって、前記ビット列 W_1 及び前記ビット列 W_2 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、

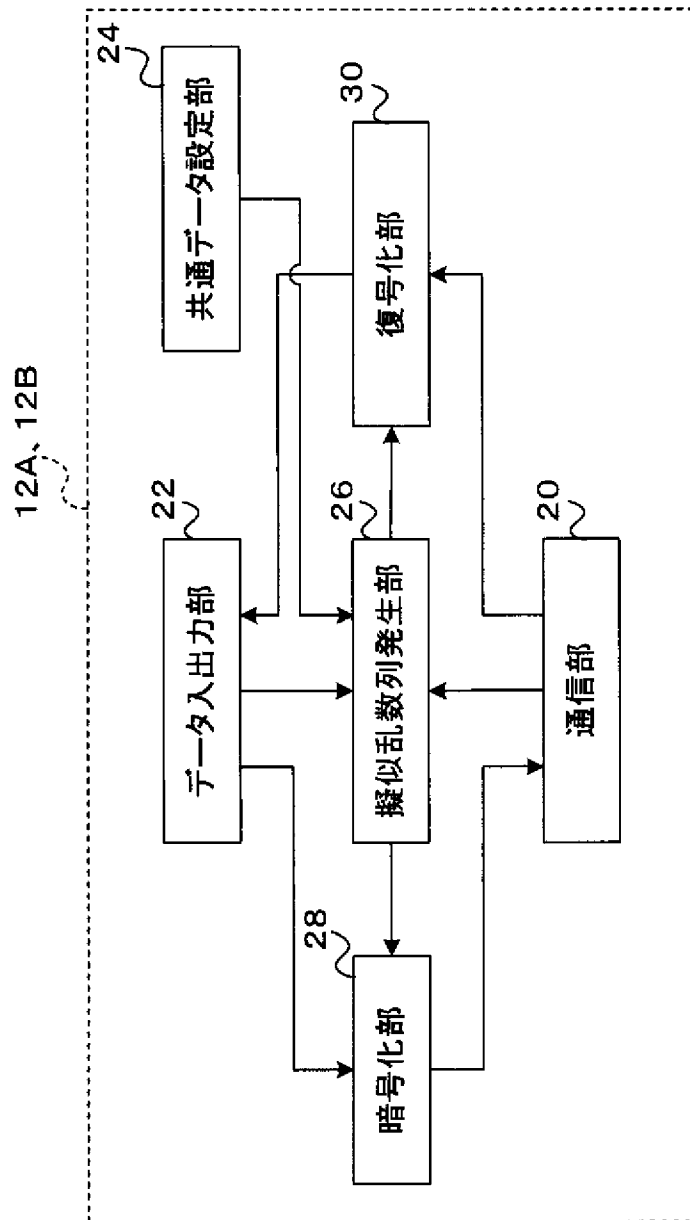
復号化部によって、前記擬似乱数列発生部によって求められた擬似乱数ビット列と、前記復号化対象データを表わすビット列との排他的論理和を計算することにより、前記復号化対象データを復号化するス

テップと
を含む復号化方法。

[図1]



[図2]



[図3A]

暗号化

Plaintext	XOR	Key	→	cyphertext
0101011	⊕	1100110	→	1011101

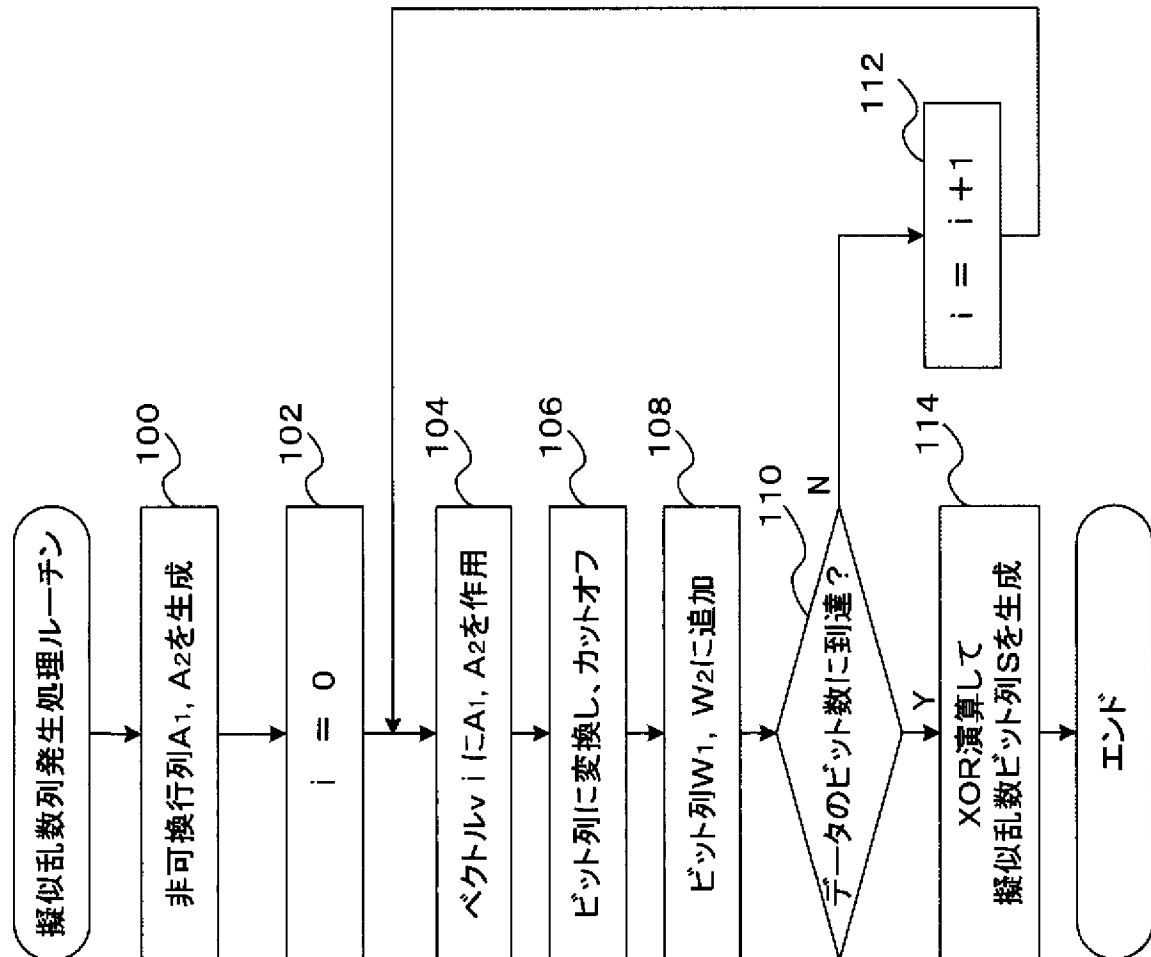
[図3B]

復号化

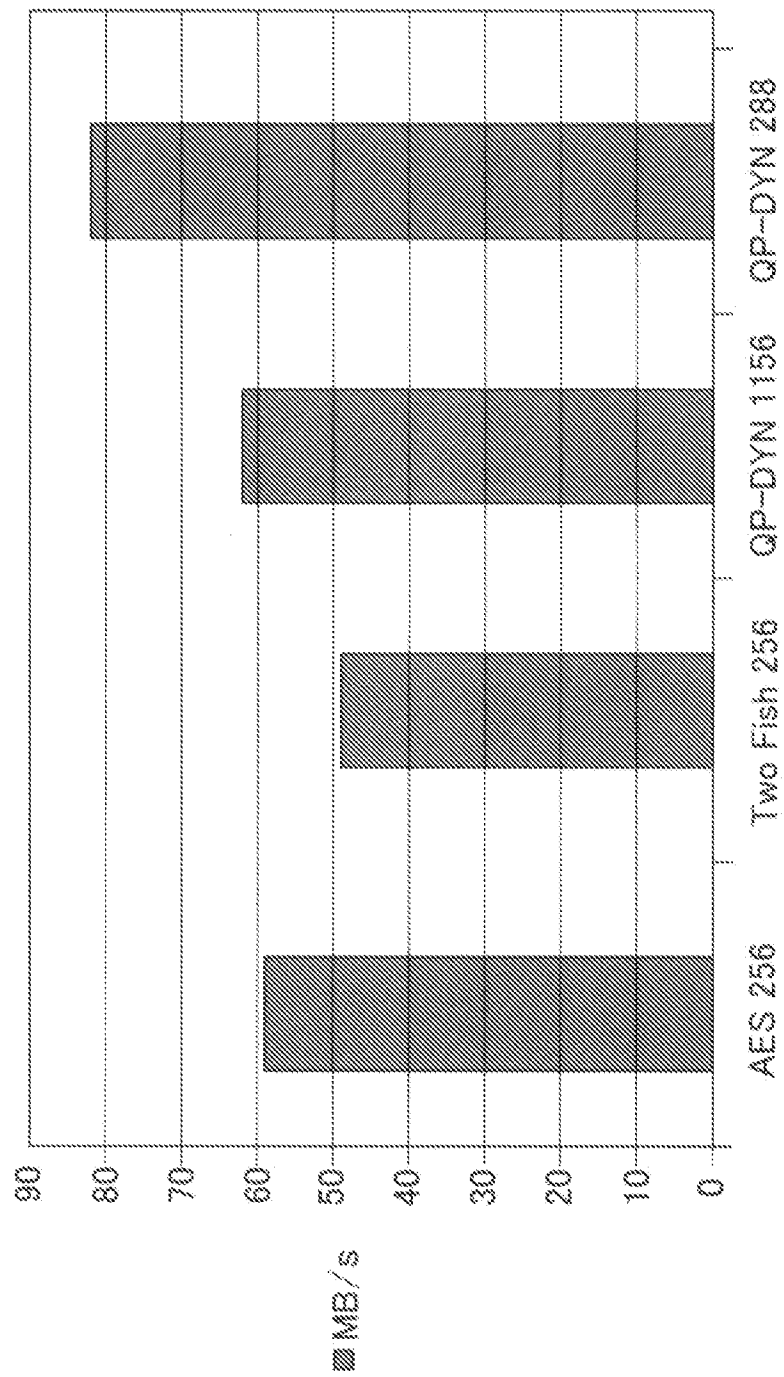
Cyphertext XOR Key → plaintext

1011101 ⊕ 1100110 → 0101011

[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2013/057509

A. CLASSIFICATION OF SUBJECT MATTER

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)

H04L9/20

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)

JSTPlus/JMEDPlus/JST7580(JDreamII), IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	M. Abundo et al, Hyperbolic automorphisms of tori and pseudo-random sequences, CALCOLO, 1992.09.01, Volume 29, Issue 3-4, p.213-240	1-9
A	Accardi, L et al, The QP-DYN algorithms, [online], 2011, [retrieval date 08 April 2013 (08.04.2013)], internet <URL:http://www.cryptalarm.it/ca/documenti/upload2set/8125_chap01.pdf>	1-9
A	JP 2001-358709 A (Casio Computer Co., Ltd.), 26 December 2001 (26.12.2001), paragraphs [0030] to [0041]; fig. 1 to 6 (Family: none)	1-9



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

08 April, 2013 (08.04.13)

Date of mailing of the international search report

16 April, 2013 (16.04.13)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2013/057509

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-264147 A (Fukuoka Institute of Technology), 11 October 2007 (11.10.2007), paragraphs [0026] to [0054]; fig. 1 to 5 (Family: none)	1-9

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. 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. H04L9/20

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)

JSTPlus/JMEDPlus/JST7580(JDreamII), IEEE Xplore

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	M. Abundo et al, Hyperbolic automorphisms of tori and pseudo-random sequences, CALCOLO, 1992.09.01, Volume 29, Issue 3-4, p.213-240	1-9
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>	1-9

☒ 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

08.04.2013

国際調査報告の発送日

16.04.2013

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)

松平 英 一

5S

3146

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
A	JP 2001-358709 A (カシオ計算機株式会社) 2001.12.26, 段落【0030】－【0041】、【図1】－【図6】 (ファミリーなし)	1－9
A	JP 2007-264147 A (学校法人福岡工業大学) 2007.10.11, 段落【0026】－【0054】、【図1】－【図5】 (ファミリーなし)	1－9