(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
2015 年 11 月 5 日(05.11.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/166701 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) *H04L 9/18* (2006.01)

(21) 国際出願番号: PCT/JP2015/055603

(22) 国際出願日: 2015 年 2 月 26 日(26.02.2015)

(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 2014-092261 2014 年 4 月 28 日(28.04.2014) JP

(72) 発明者; および
(71) 出願人 : 加沢 一郎(**KAZAWA Ichiro**) [JP/JP]; 〒1530065 東京都目黒区中町２丁目３９番１２号 Tokyo (JP).

(74) 代理人: 栗原 潔(**KURIHARA Kiyoshi**); 〒1510064 東京都渋谷区上原２－３２－３ Ｙ－２ ４０２ Tokyo (JP).

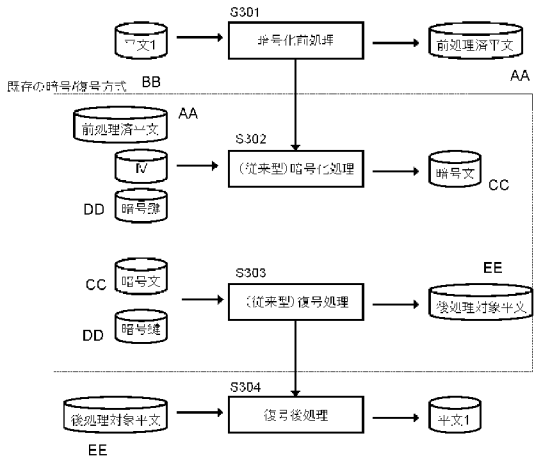
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, 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).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: ENCRYPTION METHOD, PROGRAM, AND SYSTEM

(54) 発明の名称 : 暗号化方法、プログラム、および、システム



1 Plain text
S301 Pre-process before encryption
S302 Encryption process (of conventional type)
S303 Decryption process (of conventional type)
S304 Post-process after decryption
AA Pre-processed plain text
BB Existing encryption/decryption scheme
CC Encrypted text
DD Encryption key
EE Plain text to be post-processed

(57) **Abstract**: [Problem] To perform, by use of an existing encryption scheme, an encryption that is excellent in encoding rate and suitable for stream encryption and that exhibits a high security against known plain text attacks. [Solution] From a random number sequence matrix consisting of random number sequences having no mutual correlations and having different lengths, a random number sequence is selected by using, as an index, a random number that is independently generated by means of a physical random number or the like. A plain text to be encrypted is then camouflaged on the basis of the selected random number sequence, further coupled to the aforementioned random number and thereafter subjected to application of a conventional type of encryption algorithm.

(57) 要約: 課題 : 既存の暗号化方式を利用し、符号化率が良好であり、ストリーム暗号に適した、既知平文攻撃に対して安全性が高い暗号化を行なう。 解決手段 : 互いに相関関係にない長さの異なる乱数列から成る乱数列マトリックスから、物理乱数等の手段により独立して生成された乱数をインデックスとしてひとつの乱数列を選択し、当該乱数列に基づいて暗号化対象の平文を迷彩化し、さらに、前記乱数と連結した後に従来型の暗号化アルゴリズムを適用する。

WO 2015/166701 A1

明　細　書

発明の名称 ： 暗号化方法、プログラム、および、システム

技術分野

[0001] 本発明はコンピューターによる暗号化の方法、特に、既知平文攻撃に対して安全性が高い暗号化の方法に関する。

背景技術

[0002] 今日の情報通信技術において暗号化技術はきわめて重要である。暗号化技術では、さまざまな暗号解読手法に対して安全であること、すなわち、暗号鍵の入手なしに現実的な計算時間で暗号文から平文を得られるようなことがないことが求められる。

[0003] 暗号解読手法のひとつに既知平文攻撃がある。これは、既知の特定の平文に対応する暗号文を入手できる場合に、その他の暗号文から対応する平文を求める攻撃である。通信プロトコルの標準等に基づいて平文データの最初の部分が固定、通番、あるいは、タイムスタンプ等である場合には、暗号文に対応する平文が推測しやすいため、既知平文攻撃に対する安全性は暗号化方式における重要な要件である。

[0004] 暗号化鍵の長さを単に長くするだけでは、既存の業界標準との整合性や計算量の点で課題がある。業界標準の暗号化方式に基づいて、既知平文攻撃に対する安全性を強化できることが望ましい。

[0005] また、符号化率を極端に悪化させないこと、すなわち、平文と比較した暗号文の情報量が極端に大きくならないことも必要である。

[0006] さらに、今日の情報通信技術の環境では、不定長のデータ（たとえば、デジタル化した電話音声）の暗号化も求められるため、ブロック暗号だけではなく、ストリーム暗号にも対応できることが望ましい。

[0007] 平文・初期化ベクトル・暗号化鍵などの外部入力とは独立した秘密情報を個々の暗号化の前処理として適用することにより、複数の平文暗号文ペアを情報源として用いる既知平文攻撃における計算量を増加させ、安全性を強化す

ることが可能である。

[0008] たとえば、特許文献１では、平文の全ビットを元にした秘密情報により平文を隠蔽する方法が開示されている。

[0009] しかし、特許文献１に係る方法では、ストリーム暗号に適用する場合に、適用するメモリ領域を全てキャッシュとして保持して、それの領域全体を二回走査する必要があるため、膨大な記憶容量を必要とする可能性があるという課題がある。

先行技術文献

特許文献

[0010] 特許文献1：米国特許出願公開第２００３／０１９１９５０号明細書

発明の概要

発明が解決しようとする課題

[0011] 符号化率が良好であり、ストリーム暗号に適した、既知平文攻撃に対して安全性が高い暗号化方式、システム、および、プログラムを提供する。

課題を解決するための手段

[0012] 本願発明は、乱数を生成するステップと、互いに相関関係にない長さの異なる乱数列の集合から、前記乱数に基づいてひとつの乱数列を選択するステップと、前記選択されたひとつの乱数列に基づいて第一の平文を第一の変換方法により変換するステップと、前記乱数と前記変換後の第一の平文を連結して第二の平文を作成するステップと、前記第二の平文を第二の変換方法により変換するステップとを含む暗号文作成方法を提供することで上記課題を解決する。

[0013] また、本願発明は、前段に加えて、前記第一の変換方法は、前記選択されたひとつの乱数列をくり返し連結した乱数列と前記第一の平文との排他的論理和演算である暗号文作成方法を提供することで上記課題を解決する。

[0014] また、本願発明は、乱数を生成する手順と、互いに相関関係にない長さの異なる乱数列の集合から、前記乱数に基づいてひとつの乱数列を選択する手順

と、前記選択されたひとつの乱数列に基づいて第一の平文を第一の変換方法により変換する手順と、前記乱数と前記変換後の第一の平文を連結して第二の平文を作成する手順と、前記第二の平文を第二の変換方法により変換する手順とをコンピューターに実行させる暗号文作成プログラムを提供することで上記課題を解決する。

[0015] また、本願発明は、前段に加えて、前記第一の変換方法は、前記選択されたひとつの乱数列をくり返し連結した乱数列と前記第一の平文との排他的論理和演算である暗号文作成プログラムを提供することで上記課題を解決する。

[0016] また、本願発明は、乱数を生成する手段と、互いに相関関係にない長さの異なる乱数列の集合から、前記乱数に基づいてひとつの乱数列を選択する手段と、前記選択されたひとつの乱数列に基づいて第一の平文を第一の変換方法により変換する手段と、前記乱数と前記変換後の第一の平文を連結して第二の平文を作成する手段と、前記第二の平文を第二の変換方法により変換する手段とを含む暗号文作成システムを提供することで上記課題を解決する。

[0017] また、本願発明は、前段に加えて、前記第一の変換方法は、前記選択されたひとつの乱数列をくり返し連結した乱数列と前記第一の平文との排他的論理和演算である暗号文作成システムを提供することで上記課題を解決する。

発明の効果

[0018] 従来型の暗号化方式と組み合わせることで、符号化率が良好であり、ストリーム暗号に適した、既知平文攻撃に対して安全性が高い暗号化方式、システム、および、プログラムを提供することができる。

図面の簡単な説明

[0019] [図1]本願発明の一実施形態に係る情報システムの構成図である。

[図2]本願発明の一実施形態に係る乱数列マトリックスの例である。

[図3]本願発明の一実施形態に係る暗号化および復号化処理の全体を表わすフローチャートである。

[図4]本願発明の一実施形態に係る暗号化の前処理を表わすフローチャートである。

[図5]本願発明の一実施形態に係る復号の後処理を表わすフローチャートである。

発明を実施するための形態

[0020] 以下、図を参照しながら、本願発明の実施形態の一例について説明する。

[0021] 図１は、本願発明の一実施形態に係る情報システム（101）の機能構成図である。当該情報システム（101）、および、その各機能は、一般的なコンピューター機器を使用して実現可能である。コンピューター機器はクラウドサービス等によって提供される仮想コンピューティング資源であってよい。

[0022] 暗号化前処理機能（102）は、従来型暗号化処理機能（103）に先だって変換処理を行なう機能である。当該処理の内容は図４に示されており、後述する。

[0023] 従来型暗号化処理機能（103）は、一般的な暗号化方法（たとえば、DES）による暗号化（平文から暗号文への変換）を行なう機能である。当該機能は周知技術であるためこれ以上の説明は行なわない。

[0024] 従来型復号処理機能（104）は、一般的な暗号化方法（たとえば、DES）による復号（暗号文から平文への変換）を行なう機能である。当該機能は周知技術であるためこれ以上の説明は行なわない。

[0025] 復号後処理機能（105）は、従来型復号処理機能（104）の後の処理を行なう機能である。当該処理の内容は図５に示されており、後述する。

[0026] 平文（106）は、本願発明に係る暗号化処理の入力、あるいは、復号処理の出力となるデータである。ハードディスクなどの不揮発性の記憶領域に保存されていてもよく、メインメモリ上の一時データであってもよい。また、本願発明に係る情報システム（101）の外部の情報システムから直接供給される形態でもよい。

[0027] 暗号文（107）は、本願発明に係る暗号化処理の出力、あるいは、復号処理の入力となるデータである。ハードディスクなどの不揮発性の記憶領域に保存されていてもよく、メインメモリ上の一時データであってもよい。本願発明に係る情報システム（101）が外部の情報システムに直接供給する形態でもよ

い。

[0028] 乱数列マトリックス（108）は、暗号化前処理機能（102）および復号後処理機能（105）で使用されるパラメーターである乱数列を保存する手段である。不揮発性の記憶領域に保存されていてもよく、メインメモリ上の一時データであってもよい。また、本願発明に係る情報システム（101）の外部のシステムから直接供給されてもよい。乱数列マトリックス（108）の内容は図２に示されており、後述する。

[0029] 図２は、本願発明の一実施形態に係る乱数列マトリックス（108）の例である。2^n（ここで、nは自然数）種類の互いに独立した乱数列の集合を仕様として定める。当該仕様は、誰でも入手可能な公開仕様として定めてもよく、通信を行なう当事者間で事前に交換するようにしてもよい。乱数列インデックスを指定することで、乱数列マトリックス中の特定の乱数列を指定することができる。

[0030] なお、乱数列の長さが固定であると、その固定長に相当する周期に注目することで乱数性を排除できてしまう可能性があるため、それぞれの乱数列の長さは異なり、かつ、互いに素であることが望ましい。

[0031] 図３は、本願発明の一実施形態に係る暗号化処理および復号処理をの全体像を表わすフローチャートである。各処理ステップを表わす長方形の左側に位置するデータ項目はその処理ステップの入力を表わし、右側に位置するデータ項目はその処理ステップの出力を表わす（以下同様）。本願発明に係る暗号化処理は、暗号化前処理（S301）と一般に使用されている暗号化処理（S302）（たとえば、DES）の組み合わせとして行なわれるものである。また、本願発明に係る復号処理は、一般に使用されている復号処理（S303）（たとえば、DES）と復号後処理（S304）の組み合わせとして行なわれるものである。

[0032] 図４は、本願発明の一実施形態に係る暗号化前処理（S301）の詳細を表わすフローチャートである。以下、各処理ステップについて説明する。

[0033] （S401）

nビットの乱数を平文・初期化ベクトル・暗号鍵・時刻とは無関係に自動的に

決定する。これにより、同じ条件下でも乱数は独立して決定され、2^-nの確率でしか偶然の一致はあり得なくなる。このような乱数は、たとえば、物理乱数により実現可能である。決定した乱数を乱数インデックスとして一時的に保存する。

[0034] (S402)

乱数列マトリックス（108）から、S401で求めた乱数列インデックスに対応する乱数列を求め、一時的に保存する。

[0035] (S403)

S402で求めた乱数列を使用して平文を変換し迷彩文を求める。この変換（難読化）アルゴリズムは、その逆変換が容易であること、および、データサイズを増加させないことが望ましい。たとえば、これらの条件を満足する方法として、乱数列を平文のデータ長に合うよう反復した上で、平文との排他的論理和演算を行なうことが望ましい。

[0036] (S404)

S403で得られた迷彩文と乱数列インデックスを連結して、従来型の暗号処理（S302）の対象となる平文（前処理済平文）とする。ここで、連結には、迷彩文の先頭に乱数インデックスを連結する処理、迷彩文の末尾に乱数インデックスを連結する処理、あるいは、迷彩文の所定の位置に乱数インデックスを埋め込む処理を含むものとする。前処理済平文は元々の平文と比較してデータ量が増すが、その増分は平文サイズの大小にかかわらず、乱数列インデックスのビット幅のみに限定され、符号化率を大きく悪化させることはない。

[0037] 図５は、本願発明の一実施形態に係る復号後処理（S304）の詳細を表わすフローチャートである。以下、各処理ステップについて説明する。

[0038] (S501)

従来型復号処理方法（たとえば、DES）により復号された後処理対象平文を分離し、乱数列インデックスと迷彩文を得る。乱数列インデックスの長さ、および、挿入位置は仕様として定まっているため、この処理の内容は自明であ

る。

[0039] (S502)

乱数列マトリックス（108）において、S501で求めた乱数列インデックスに対応する乱数列を求め一時的に保存する。

[0040] (S503)

S502で求めた乱数列を使用して迷彩文を変換し平文を求める。この変換処理は、S403で行なわれた処理の逆変換である。たとえば、S403で乱数列を必要な回数繰り返して、排他的論理和演算を行なったのであれば、同じ演算を再度行なえばよい。

[0041] （本方式による暗号化の安全性の説明）

以下に、本願発明に係る暗号化方式の既知平文攻撃に対する安全性の高さについて説明する。

[0042] 乱数列インデックスは処理内における独自の乱数源から生成され、最終的に暗号化されることにより秘匿性が保証される。どの乱数列インデックスが使用されるかは推測も強制も不可能である。以下では、乱数列インデックスのビット幅をnとし、既知平文攻撃で必要な平文暗号文ペアの個数をmとし、暗号化で使用する鍵のビット幅をLとする。

[0043] 既知平文攻撃による攻撃者が、複数の平文と暗号文ペアを所有している場合でも、各ペアは独立した乱数列インデックスを持つ。従って、複数の平文暗号文ペアを処理する場合には、(2^n)^m = 2^(n*m)種類の組み合わせを総当りする必要がある。一方、全数検索（総当たり方式）での処理回数は 2^L 回である。

[0044] 全数検索における一回のチェック実行の処理内容は、復号して確認することのみである。一方、既知平文攻撃では、一回のチェック実行の処理内容は、上記の処理に加えて、組み合わせで得たペアで鍵を解読する処理から成る。ゆえに、全数検索での１回あたりのチェック処理時間をT1、既知平文攻撃での１回あたりのチェック処理時間をT2とすると、T1＜＝T2である。

[0045] 既知平文攻撃が成功するということは、全数検索よりも速く鍵を特定できる

ことを意味する。計算量の総計は、実行あたりの計算量に計算回数を掛けたものであることから、既知平文攻撃が成功するという条件は T1 * 2^L > T2 * 2^(n*m) という不等式で表わされる。

[0046] T1 <= T2 により T1 * 2^L > T2 * 2^(n*m) は、以下の通り、2^L > 2^(n*m) に変形される。

T1 * 2^L > T2 * 2^(n*m)

→ T1/T2 * 2^L > 2^(n*m)

→ (1 >= T1/T2 なので) 1 * 2^L >= T1/T2 * 2^L > 2^(n*m)

→ 2^L > 2^(n*m)

そしてmの条件を掃き出すと、以下の通り、L/n > m となる。

2^L > 2^(n*m)

→ (L>0, n>0, m>0 なので) Log(2^L) > Log(2^(n*m))

→ L * Log(2) > n * m * Log(2)

→ L > n * m

→ L/n > m

[0047] 例えば乱数列インデックスが8ビットという取り決めの元に本発明に係る暗号化方法を適用すると、既知平文攻撃が成功したとみなされる条件は、鍵長が256ビットの暗号では、32個未満の平文暗号文ペアで解読できた場合であり、鍵長が56ビットの暗号では既知平文攻撃を行う場合、7個未満の平文暗号文ペアで解読できた場合である。

[0048] 現状の既知平文攻撃において、平文暗号文ペアの個数は処理量とは相関しないと考えられているため、理論的な上限はないが、本発明は、平文暗号文ペアの個数に明確な制限を課すことができる点で有利である。

[0049] （本発明の技術的に顕著な効果）

本発明は、従来型の一般的暗号化方式との組み合わせにより容易に実現できる一方で、符号化率が良好であり、平文を複数回走査する必要がないためストリーム暗号においても利用しやすく、加えて、従来型暗号化方式の暗号鍵の長さが仕様により固定されている場合でも本発明に係る方式を追加するこ

とで、暗号化方式全体としての強度、とりわけ、既知平文攻撃に対する安全性を強化できる。

請求の範囲

[請求項1] 乱数を生成するステップと、
互いに相関関係にない長さの異なる乱数列の集合から、前記乱数に基づいてひとつの乱数列を選択するステップと、
前記選択されたひとつの乱数列に基づいて第一の平文を第一の変換方法により変換するステップと、
前記乱数と前記変換後の第一の平文を連結して第二の平文を作成するステップと、
前記第二の平文を第二の変換方法により変換するステップとを
含む暗号文作成方法。

[請求項2] 前記第一の変換方法は、前記選択されたひとつの乱数列をくり返し連結した乱数列と前記第一の平文との排他的論理和演算である請求項１に記載の暗号文作成方法。

[請求項3] 乱数を生成する手順と、
互いに相関関係にない長さの異なる乱数列の集合から、前記乱数に基づいてひとつの乱数列を選択する手順と、
前記選択されたひとつの乱数列に基づいて第一の平文を第一の変換方法により変換する手順と、
前記乱数と前記変換後の第一の平文を連結して第二の平文を作成する手順と、
前記第二の平文を第二の変換方法により変換する手順とを
コンピューターに実行させる含む暗号文作成プログラム。

[請求項4] 前記第一の変換方法は、前記選択されたひとつの乱数列をくり返し連結した乱数列と前記第一の平文との排他的論理和演算である請求項３に記載の暗号文作成プログラム。

[請求項5] 乱数を生成する手段と、
互いに相関関係にない長さの異なる乱数列の集合から、前記乱数に基づいてひとつの乱数列を選択する手段と、

前記選択されたひとつの乱数列に基づいて第一の平文を第一の変換方法により変換する手段と、

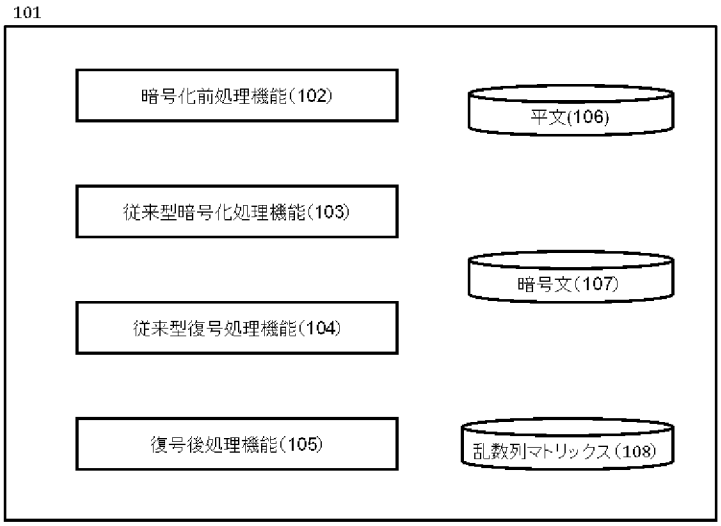
前記乱数と前記変換後の第一の平文を連結して第二の平文を作成する手段と、

前記第二の平文を第二の変換方法により変換する手段とを

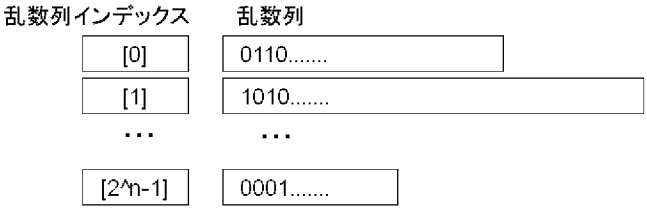
含む暗号文作成システム。

[請求項6] 前記第一の変換方法は、前記選択されたひとつの乱数列をくり返し連結した乱数列と前記第一の平文との排他的論理和演算である請求項５に記載の暗号文作成システム。

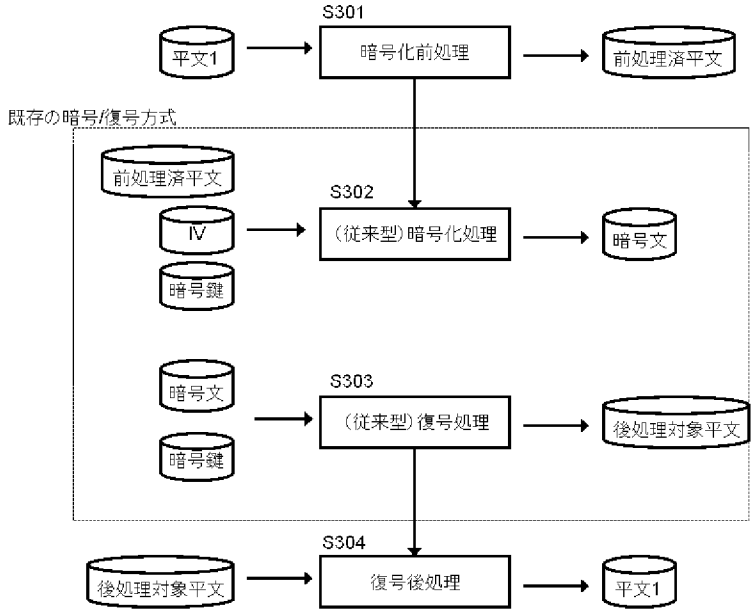
[図1]


101
暗号化前処理機能(102)
平文(106)
従来型暗号化処理機能(103)
暗号文(107)
従来型復号処理機能(104)
復号後処理機能(105)
乱数列マトリックス(108)

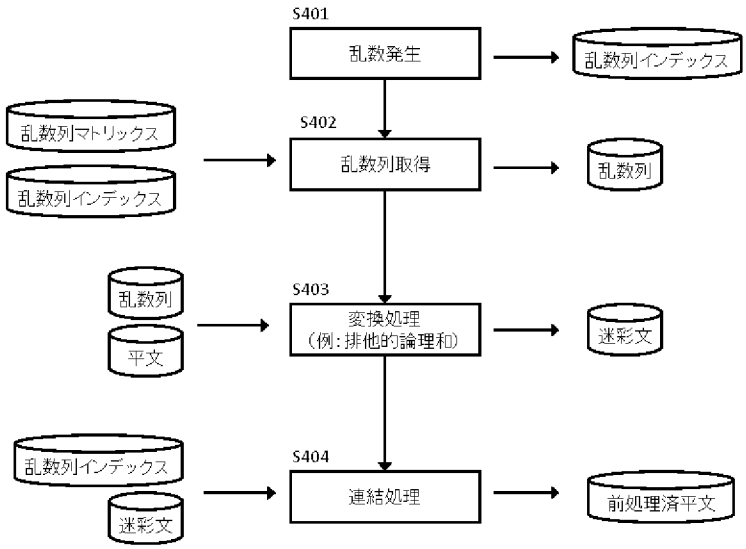
[図2]


乱数列インデックス
乱数列
[0]
0110.....
[1]
1010.....
...
...
[2^n-1]
0001.....

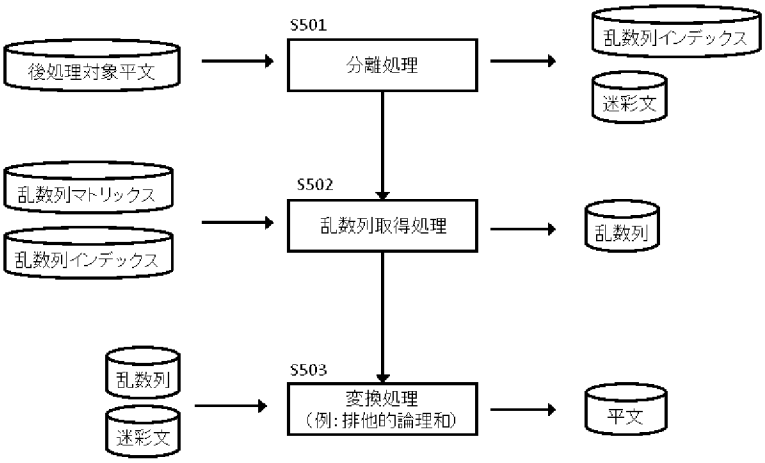
[図3]


S301
平文1
暗号化前処理
前処理済平文
既存の暗号/復号方式
前処理済平文
IV
暗号鍵
S302
(従来型)暗号化処理
暗号文
暗号文
暗号鍵
S303
(従来型)復号処理
後処理対象平文
S304
後処理対象平文
復号後処理
平文1

[図4]


S401
乱数発生
乱数列インデックス
乱数列マトリックス
乱数列インデックス
S402
乱数列取得
乱数列
乱数列
平文
S403
変換処理
(例:排他的論理和)
迷彩文
乱数列インデックス
迷彩文
S404
連結処理
前処理済平文

[図5]


S501
後処理対象平文
分離処理
乱数列インデックス
迷彩文
乱数列マトリックス
乱数列インデックス
S502
乱数列取得処理
乱数列
乱数列
迷彩文
S503
変換処理
（例：排他的論理和）
平文

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/055603

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/14(2006.01)i, *H04L9/18*(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)
H04L9/14, H04L9/18

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	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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	WO 2008/114829 A1 (Tokyo Denki University), 25 September 2008 (25.09.2008), paragraphs [0015] to [0019]; fig. 1 & JP 4737334 B	1-6
Y	Anand Desai, New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack, Advances in Cryptology - CRYPTO 2000, 2000, pp. 394-412	1-6
Y	JP 11-331619 A (Oki Data Corp.), 30 November 1999 (30.11.1999), paragraph [0008] (Family: none)	2,4,6

☐ 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
30 March 2015 (30.03.15)	07 April 2015 (07.04.15)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／０５５６０３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14(2006.01)i, H04L9/18(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.　H04L9/14, H04L9/18

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	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５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	WO 2008/114829 A1（学校法人東京電機大学）2008.09.25, 段落［００１５］－［００１９］, 図１ & JP 4737334 B	1-6
Y	Anand Desai, New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack, Advances in Cryptology - CRYPTO 2000, 2000, pp. 394-412	1-6
Y	JP 11-331619 A（株式会社沖データ）1999.11.30, 段落［０００８］(ファミリーなし)	2, 4, 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
３０．０３．２０１５	０７．０４．２０１５

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　４４４０
打出　義尚
電話番号　０３－３５８１－１１０１　内線　３５４６