(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-295507
(P2005-295507A)
(43)公開日　平成17年10月20日(2005.10.20)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/22	H04L	9/00　655	5J104

審査請求 未請求　請求項の数 40　ＯＬ　（全 20 頁）

(21)出願番号　特願2005-33533(P2005-33533)
(22)出願日　平成17年2月9日(2005.2.9)
(31)優先権主張番号　10/815,572
(32)優先日　平成16年3月31日(2004.3.31)
(33)優先権主張国　米国(US)

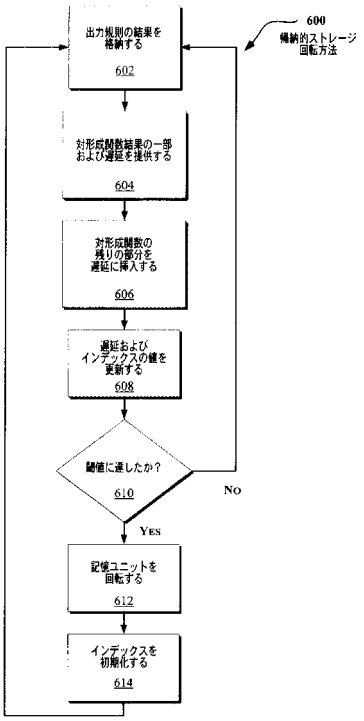
（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　イリヤ　ミロノフ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】回転バッファを用いたストリーム暗号設計

(57)【要約】
【課題】　ストリーム暗号のキーストリームジェネレータの出力に関連する短期的相関を制限するための技術を提供すること。
【解決手段】　ジェネレータの出力値が、対をなす出力が互いに独立していると見なされるほど十分に離れているように対にされる。説明する一実施形態では、方法が、ストリーム暗号出力規則によってもたらされた複数の結果を第１、第２および第３の記憶ユニットに順次格納することを含む。対形成関数によって、少なくとも閾値だけ離れた第１および第３の記憶ユニットからの個々の値を対にする。出力規則の結果の閾値に達すると、第１、第２および第３の記憶ユニットの内容が順次回転される。
【選択図】　図６



【特許請求の範囲】
【請求項１】
ストリーム暗号出力規則によってもたらされた複数の結果を第１、第２および第３の記憶ユニットに順次格納するステップと、
少なくとも閾値だけ離れた前記第１および第３記憶ユニットからの個々の値を対にする対形成関数から複数の結果を提供するステップと、
前記出力規則の前記閾値に達すると、前記第１、第２および第３記憶ユニットの内容を順次回転するステップと
を含むことを特徴とする方法
【請求項２】
前記第１および第３記憶ユニットからの前記個々の値の間の短期的相関が制限されることを特徴とする請求項１に記載の方法。
【請求項３】
前記第１、第２および第３記憶ユニットのそれぞれの長さは前記閾値に等しいことを特徴とする請求項１に記載の方法。
【請求項４】
前記第１、第２および第３記憶ユニットが単一のメモリ装置内で実装されることを特徴とする請求項１に記載の方法。
【請求項５】
前記順次回転は、前記第１、第２および第３記憶ユニットを同じ方向にシフトすることによって実行されることを特徴とする請求項１に記載の方法。
【請求項６】
前記対形成関数の結果がテーブル内に格納されることを特徴とする請求項１に記載の方法。
【請求項７】
ストリーム暗号キーストリームジェネレータの出力を強化するために使用されることを特徴とする請求項１に記載の方法。
【請求項８】
所与の任意の時点において前記第１および第３記憶ユニットだけがアクティブであることを特徴とする請求項１に記載の方法。
【請求項９】
前記第１および第３記憶ユニットだけがランダム値で初期化されることを特徴とする請求項１に記載の方法。
【請求項１０】
請求項１に記載の方法が繰り返し実行されることを特徴とする請求項１に記載の方法。
【請求項１１】
前記出力規則が、ランダムウォーク、Ｔ関数、ＬＦＳＲ（線形フィードバックシフトレジスタ）およびワードベースのストリーム暗号を含むグループから選択された１つまたは複数の更新規則と組み合わせられることを特徴とする請求項１に記載の方法。
【請求項１２】
前記ランダムウォークが、加法型ウォーク、乗法型ウォーク、ガバーガリル型ウォーク、ラマヌジャン型ウォーク、置換型ウォーク、および動的ジェネレータを用いたランダムウォークを含むグループ内の１つまたは複数のウォークから選択されることを特徴とする請求項１１に記載の方法。
【請求項１３】
第４の記憶ユニットを使用することによって前記対形成関数を強化するステップをさらに含むことを特徴とする請求項１に記載の方法。
【請求項１４】
前記第４記憶ユニットが、１サイクルの秘密の置換を使用することによってウォークスルーされることを特徴とする請求項１３に記載の方法。

【請求項１５】
前記秘密の置換は緩やかに変化することを特徴とする請求項１４に記載の方法。
【請求項１６】
前記第４記憶ユニットがランダム値で初期化されることを特徴とする請求項１３に記載の方法。
【請求項１７】
前記第４記憶ユニットがランダム値および可変遅延で初期化されることを特徴とする請求項１３に記載の方法。
【請求項１８】
プロセッサと、
前記プロセッサに結合されたシステムメモリとを含むシステムであって、
ストリーム暗号出力規則によってもたらされた複数の結果を前記システムメモリの第１、第２および第３の部分に順次格納し、
少なくとも閾値だけ離れた前記システムメモリの前記第１および第３の部分からの個々の値を対にする対形成関数から複数の結果を提供し、
前記出力規則の前記閾値に達すると、前記システムメモリの前記第１、第２および第３の部分の内容を順次回転する
ことを特徴とするシステム。
【請求項１９】
前記システムメモリの前記第１および第３の部分からの前記個々の値の間の短期的相関が制限されることを特徴とする請求項１８に記載のシステム。
【請求項２０】
前記システムメモリの前記第１、第２および第３の部分のそれぞれの長さは前記閾値に等しいことを特徴とする請求項１８に記載のシステム。
【請求項２１】
前記第１、第２および第３の部分が複数のメモリ装置内で実装されることを特徴とする請求項１８に記載のシステム。
【請求項２２】
前記順次回転は、前記第１、第２および第３の部分を同じ方向にシフトすることによって実行されることを特徴とする請求項１８に記載のシステム。
【請求項２３】
前記対形成関数の結果が前記システムメモリのテーブル内に格納されることを特徴とする請求項１８に記載のシステム。
【請求項２４】
ストリーム暗号キーストリームジェネレータの出力を強化するために使用されることを特徴とする請求項１８に記載のシステム。
【請求項２５】
前記第１および第３の部分がランダム値で初期化されることを特徴とする請求項１８に記載のシステム。
【請求項２６】
前記出力規則が、ランダムウォーク、Ｔ関数、ＬＦＳＲ（線形フィードバックシフトレジスタ）およびワードベースのストリーム暗号を含むグループから選択された１つまたは複数の更新規則と組み合わせられることを特徴とする請求項１８に記載のシステム。
【請求項２７】
前記ランダムウォークが、加法型ウォーク、乗法型ウォーク、ガバーガリル型ウォーク、ラマヌジャン型ウォーク、置換型ウォーク、および動的ジェネレータを用いたランダムウォークを含むグループ内の１つまたは複数のウォークから選択されることを特徴とする請求項２６に記載のシステム。
【請求項２８】
前記対形成関数の操作が前記システムメモリの第４の部分を使用することによって強化

されることを特徴とする請求項１８に記載のシステム。
【請求項２９】
前記第４の部分がランダム値で初期化されることを特徴とする請求項２８に記載のシステム。
【請求項３０】
前記第４の部分がランダム値および可変遅延で初期化されることを特徴とする請求項２８に記載のシステム。
【請求項３１】
実行された場合にマシンに、
ストリーム暗号出力規則によってもたらされた複数の結果を第１、第２および第３の記憶ユニットに順次格納するステップと、
少なくとも閾値だけ離れた前記第１および第３記憶ユニットからの個々の値を対にする対形成関数から複数の結果を提供するステップと、
前記出力規則の前記閾値に達すると、前記第１、第２および第３の記憶ユニットを順次回転するステップと
を含む行為を実行するように指示する命令が格納されていることを特徴とする１つまたは複数のコンピュータ読取り可能媒体。
【請求項３２】
前記第１および第３記憶ユニットからの前記個々の値の間の短期的相関が制限されることを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３３】
前記第１、第２および第３記憶ユニットのそれぞれの長さは前記閾値に等しいことを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３４】
前記第１、第２および第３記憶ユニットが単一のメモリ装置内で実装されることを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３５】
前記順次回転は、前記第１、第２および第３記憶ユニットを同じ方向にシフトすることによって実行されることを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３６】
前記対形成関数の結果がテーブル内に格納されることを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３７】
前記行為が繰り返し実行されることを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３８】
前記出力規則が、ランダムウォーク、Ｔ関数、ＬＦＳＲ（線形フィードバックシフトレジスタ）およびワードベースのストリーム暗号を含むグループから選択された１つまたは複数の更新規則と組み合わせられることを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項３９】
前記ランダムウォークが、加法型ウォーク、乗法型ウォーク、ガバーガリル型ウォーク、ラマヌジャン型ウォーク、置換型ウォーク、および動的ジェネレータを用いたランダムウォークを含むグループ内の１つまたは複数のウォークから選択されることを特徴とする請求項３８に記載の１つまたは複数のコンピュータ読取り可能媒体。
【請求項４０】
第４の記憶ユニットを使用することによって前記対形成関数を強化するステップをさらに含むことを特徴とする請求項３１に記載の１つまたは複数のコンピュータ読取り可能媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般には、暗号化に関し、より詳細には、ストリーム暗号に回転（ｒｅｖｏｌｖｉｎｇ，ｒｏｔａｔｉｎｇ）バッファを使用することに関する。
【背景技術】
【０００２】
デジタル通信がより一般的になるにつれて、関連する通信チャネルを安全にする必要性がますます重要になる。例えば、現在の技術は、ユーザが銀行口座、医療データ、ならびに他の私的な機密の情報にリモートでアクセスすることを可能にする。
【０００３】
安全なデジタル通信を提供するために、暗号が広く用いられてきた。暗号は一般に、メッセージの暗号化（ｅｎｃｉｐｈｅｒｉｎｇ，ｅｎｃｒｙｐｔｉｎｇ）および解読（ｄｅｃｉｐｈｅｒｉｎｇ，ｄｅｃｒｙｐｔｉｎｇ）に関する。暗号化および解読では、何らかの秘密の情報（鍵など）が使用される。様々な暗号化方法において、暗号化および解読のために、単一の鍵または複数の鍵が使用される。
【０００４】
現在、２つのタイプの暗号が一般に使用されている。ブロック暗号は、大きいデータブロックに作用する。一方、ストリーム暗号は、テキストの比較的小さい単位（ビットなど）に作用する。その実施に応じて、ストリーム暗号は、ブロック暗号より遥かに高速であり得る。
【０００５】
ストリーム暗号は、それによって生成されるストリーム（キーストリームとも称される）がワンタイムパッドまたはバーナム暗号の高い安全性に近づいているので、最近は特別な関心事になっている。一般に、ワンタイムパッド暗号は、暗号化されるテキストメッセージと同じ長さのキーストリームを生成する。ワンタイムパッドのキーストリームは、完全にランダムであり、非常に高い安全性のレベルをもたらすと考えられるが、一部の応用にとっては望ましくない場合があるメモリのオーバヘッドが生じる。
【０００６】
【非特許文献１】A. Menezes, P van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," fifth printing (August 2001), published by CRC Press
【発明の開示】
【発明が解決しようとする課題】
【０００７】
ストリーム暗号は通常、擬似乱数ジェネレータをもとに作られる。暗号は、シミュレーションに適した効率的な、統計的に有効な多くのジェネレータを支配しようとする攻撃に耐える必要がある。
【０００８】
したがって、現在の解決策は、ストリーム暗号を用いた迅速で安全なデータ暗号化／解読のための効率的な方法論を提供できていない。
【課題を解決するための手段】
【０００９】
ストリーム暗号のキーストリームジェネレータの出力に関連する短期的な相関を制限するための技術が開示される。ジェネレータの出力値は、対をなす出力が互いに独立していると見なされるほど十分に離れているように対にされる。
【００１０】
説明する一実施形態では、方法は、ストリーム暗号出力規則によってもたらされた複数の結果を第１、第２および第３の記憶ユニット内に順次格納することを含む。対形成関数（ｐａｉｒｉｎｇ　ｆｕｎｃｔｉｏｎ）は、少なくとも閾値だけ離れた第１および第３記憶ユニットからの別個の値を対にする。出力規則の結果の閾値に達すると、第１、第２お

よび第３記憶ユニットの内容が順次回転される。

【００１１】

説明する別の実施形態では、比較的単純な更新が、効率的な出力規則（対形成関数によって強化される規則など）と組み合わせられて、ストリーム暗号の構成が強化され、および／または様々な新しい暗号が構成される。

【００１２】

詳細な説明について、添付の図面を参照して述べる。図では、参照番号の最も左の桁によって、その参照番号が最初に現れる図を識別する。それぞれ異なる図中で同じ参照番号を使用することにより、類似または同一のアイテムを示す。

【発明を実施するための最良の形態】

【００１３】

以下の説明は、読者が暗号技術に精通していることを前提としている。暗号技術の基本的な序論について、非特許文献１に記載のテキストを参照されたい。

【００１４】

以下の開示では、ストリーム暗号のキーストリームジェネレータの出力に関連するローカルな（または短期的な）相関を制限するための効率的な技術について説明する。この技術は、互いに独立していると見なされるほど十分に離れているジェネレータ出力を対にすることに基づく。ある実施形態では、１つには攻撃者が変数をほとんど含まない比較的短い方程式を分離することができないという理由から、対形成グラフ（ｐａｉｒｉｎｇ ｇｒａｐｈ）内に短いサイクルが存在しないことによって、線形攻撃および代数的攻撃が実質上制限される。

【００１５】

ある実施形態では、（例えば図２を参照してさらに説明するように）比較的単純な更新（「更新規則」の節で以下に詳しく説明する）が、効率的な出力規則と組み合わせられて、（例えば、望ましい特性を有するプロセスのうちの２つ以上を組み合わせることによって）多数の既知のストリーム暗号構成が強化されおよび／または多種多様な新しい暗号が構成される。こうした実施形態は、ソフトウェアでも効率的であると考えられる。

【００１６】

ストリーム暗号概要

図１に、例示的なストリーム暗号システム１００を示す。システム１００は、キーストリームジェネレータ１０２を含む。鍵（ｋ）１０４を使用して、キーストリーム（z_i）を生成するキーストリームジェネレータ１０２を含む。生成されたキーストリーム（z_i）とメッセージ（m_i）１０８を組み合わせるために出力関数が適用されて（１０６）、暗号文（１１０）が生成される。生成されたキーストリーム（z_i）は、時間によって変化し、また最初の小さいキーストリーム（シードなど）から、シードと前の暗号文からなど、ランダムに生成される。出力関数（１０６）は、メッセージ（m_i）の個々の文字（またはビット）に１度に１つ適用される。

【００１７】

したがって、システム１００は、生成されたキーストリームを使用して、メッセージ（m_i）を暗号文（c_i）に暗号化する。ストリーム暗号アルゴリズムの典型的な設計は一般に、３つの要素からなる。

【００１８】

１．暗号の内部状態Ω_0を（例えば図１の１０４などの鍵および／またはランダム値を使用することによって）初期化するための規則。

【００１９】

２．Ｅ：Ω→Ω、すなわち状態Ωを発展させるかまたは更新する（例えばキーストリームジェネレータ１０２によって行われる）ための機構。

【００２０】

３．Ｈ：Ω→｛０，１｝^{n}、すなわちｎビット出力（図１の１０２によって生成されるキーストリーム（z_i）など）を生成するための出力規則。

【００２１】
安全で効率的な暗号を設計する際に注意深く選択されるべき多くの可能なトレードオフが存在する。具体的には、更新規則Ｅと出力規則Ｈの間には当然のトレードオフが存在する。例えば、状態の更新が非常に徹底的に行われる場合、その出力は、状態の比較的単純な関数であり、またその逆の場合も同様であり得る。
【００２２】
ある実施形態では、（例えば図２を参照してさらに説明するように）比較的単純な更新（「更新規則」の節で以下にさらに説明する）が効率的な出力規則と組み合わせられる。例えば、速い更新規則Ｅおよび単純な出力規則Ｈを用いたシナリオが与えられると、発展する規則Ｅは、長期的に有効であり、例えば規則がＴ回適用された後には、状態E^T（Ω_t）がΩ_tにほとんどまたはまったく類似しないような何らかの特徴的な時間Ｔが存在する。こうした技術は、上記の特性を有するプロセスのうちの２つ以上を組み合わせることによって、知られている多くのストリーム暗号の構成を強化することができ、または多種多様な新しい暗号を構成するために使用されることができる。こうした実施形態は、ソフトウェアでも効率的であると考えられる。
【００２３】
回転ストレージまたはバッファ
図２に、回転記憶ユニットを使用することによって出力規則Ｈを強化するための例示的な方法２００を示す。ある実施形態では、方法２００によって、キーストリームジェネレータ（図１の１０２など）によって生成されるキーストリームを向上させる。出力規則Ｈによって生成された要素（個々の文字またはビットなど）が格納される（２０２）。要素を格納するために、レジスタ、キャッシュ、または他のタイプのメモリ（例えば図７のコンピューティング環境を参照して説明するメモリ）など、様々なタイプの装置または媒体が使用される。格納されたデータは、同じ装置内に常駐することも、それぞれ異なる装置内に常駐することもある。
【００２４】
（同じ表題のもとで以下に説明する）対形成関数Ｐは、少なくとも２つの対応する記憶ユニット（図３および４に示される記憶ユニットＡおよびＣなど）内に格納された値に基づいて対形成結果を提供する（２０４）。ある実施形態では、対形成関数は、２つより多い入力を取り得る。インデックス（例えば記憶ユニットおよび／または対形成関数に索引付けするために使用される）は、例えば１だけ更新される（２０６）。例えば更新されたインデックスを閾値と比較することによって判断されるが、所与の閾値（Ｔ）に達していない場合（２０８）、この方法２００は、段階２０２に戻って、出力規則Ｈによって生成された次の要素を格納する。
【００２５】
そうでない場合、閾値に達すると（２０８）、記憶ユニットは、（例えば格納されている値を左または右にシフトすることによって）順次回転される（２１０）。ある実施形態では、効率をもたらすために回転がポインタに適用され、それによって、データの移動を回避する（例えば単に記憶ユニットが名前変更される）。ついで、インデックスが（例えば０に）初期化され（２１２）、方法２００は、段階２０２で再開して、出力規則Ｈによって生成された次の要素を格納する。方法２００は、所望の長さのキーストリームが生成されるまで実施される。
【００２６】
したがって、出力規則は、少なくともＴステップ離れている（すなわち段階２０８を参照して説明したように閾値量だけ離れている）２つの出力要素を対にする対形成関数ｐによって強化される。そうすることによって、互いにＴステップ離れて行われる内部状態の２つの観察は、実用的な目的のために、実質上無関係であると見なされる。１つの解決策は、中間の結果（段階２０２によって生成される結果など）を捨てることである。代わりに、結果は、記憶ユニット（またはバッファ）内に格納され、出力結果が適切に対にされる。結果が格納され、対にされるやり方が、この技術の効率の１つの源泉になっている。

【００２７】
ある実施形態では、所与の時点で、Ａ、ＢおよびＣ（図３）と称される、長さＴの３つの記憶ユニット（または同じ記憶ユニット内の３つの部分）が存在する。ストリーム暗号出力規則からの結果は、記憶ユニット内に順次格納される（２０２）。Ｔサイクルごとに、記憶ユニットの内容が左にシフトされ（Ａが廃棄され、ＢがＡに移動し、Ｃが空にされ）または右にシフトされる（Ｃが廃棄され、ＢがＣに移動し、Ａが空にされる）。こうした実施形態では、ＡおよびＣの配列だけがアクティブに読み出され、Ｂは、（左シフトの場合は）Ｃが一杯になるまで休止状態にある。したがって、記憶ユニットを左にシフトする場合、図２を参照して説明したように、以下のステップが反復される。
【００２８】
１．Ｃ［ｉ］←出力規則Ｈによって生成された要素（２０２）。
【００２９】
２．ｐ（Ａ［n_i］；Ｃ［ｉ］）を提供する（２０４）。
【００３０】
３．ｉ←ｉ＋１（２０６）。
【００３１】
４．ｉ＝Ｔの場合（２０８）、Ａ←Ｂ、Ｂ←Ｃ（２１０）、ｉ←０（２１２）。
【００３２】
ある実施形態では、最後の操作は、３つのバッファを指すポインタを回転させることによって効率的に実施される。ある実施形態では、方法２００の諸段階の実施に先立って、記憶ユニットＡおよびＢが（例えばランダム値、または出力関数Ｈによって生成された値によって）初期化される。
【００３３】
対形成関数ｐを定義するために、$i \in \{0, T\}$について、定数n_iのテーブル（ｉ，n_i）が定義される。第１に、$a_0, \ldots, a_{T_1}$および$c_0, \ldots, c_{T_1}$でラベル付けされた頂点を含む無向グラフ（ｕｎｄｉｒｅｃｔｅｄ　ｇｒａｐｈ）Ｇが定義される（図４）。第２に、$0 \leqq i \leqq T-1$の場合は、エッジ（a_i，a_{i+1}）および（c_i，c_{i+1}）が追加され、$0 \leqq i \leqq T$の場合は、
【００３４】
【数１】
$$(a_{n_i}, c_i)$$

【００３５】
が追加される。対（n_i，ｉ）では、グラフＧの内周（ｇｉｒｔｈ）が比較的大きい（ただし、内周は一般に、Ｇ内の最短サイクルの長さである）。対形成関数の代わりに、またはそれに加えて、複数の引数（ｍｕｌｔｉｐｌｅ　ａｒｇｕｍｅｎｔ）の関数を使用することが考えられる。さらに、その関数は、２つより多い引数（例えば各バッファから１つ）を取り得る。
【００３６】
対形成関数
対形成関数$p: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$に関して、例えばそれぞれのｘについて、関数ｙ→ｐ（ｘ，ｙ）は１対１である。同様に、それぞれのｙについて、関数ｘ→ｐ（ｘ，ｙ）も全単射である。ある実施形態では、関数は、計算上効率的であり、その入力において対称的でない。対形成関数の一部の例示的な選択肢は以下の通りである。
【００３７】
Ａ：
【００３８】

【数２】
$$p(x,y)=x\oplus S[y]$$

【００３９】
ただし、Ｓは固定の置換テーブルである。
【００４０】
Ｂ：
【００４１】
【数３】
$$p(x,y)=x\oplus(ay+b)$$

【００４２】
ただし、ａおよびｂは２つの定数であり、ａは奇数である。この操作は、（図７の処理装置７０４を参照して説明するプロセッサなど）現在のプロセッサの一部で使用可能なＳＳＥ（ストリーミングＳＩＭＤ（ｓｉｎｇｌｅ ｉｎｓｔｒｕｃｔｉｏｎ ｍｕｌｔｉｐｌｅ ｄａｔａ：単一命令複数データ）拡張）を使用して効率的に実施される。
【００４３】
以下の規則の反復によって、Ｃ：ｐ（ｘ，ｙ）＝γ，δが、ほぼ普遍的なハッシュ関数として選択される。
【００４４】
$\alpha = a x \mod 2^{2n}$
$\beta = b y \mod 2^{2n}$
$\gamma = \alpha^{L} + \beta^{R} \mod 2^{2n}$
$\delta = \alpha^{R} + \beta^{L} \mod 2^{2n}$
ただし、x^{L}およびx^{R}はｘの左半分および右半分をそれぞれ表し、ａ，ｂはランダムに選択される。
【００４５】
グラフＧは、相手方に知られている関係を概略的に反映しており、（a_i，a_{i+1}）と（c_i，c_{i+1}）は内部状態の更新によって接続され、また
【００４６】
【数４】
$$(a_{n_i}, c_i)$$

【００４７】
は対形成関数の引数である。
【００４８】
対形成関数は、その引数の両方において全単射であるので、その正確な引数を知ることによって、その引数のいずれかに関する情報は漏洩されない。関数の構成時に取消しが行われなければ、導出される最良の関係は、少なくともｋ入力（グラフの内周）を含む。実際に、任意のｍ＜ｋの出力、z_0＝対（x_0，y_0），z_1＝対（x_1，y_1），．．．，z_m＝対（x_m，y_m）では、これらの出力をもたらす多くの入力対（x_0，y_0），．．．，（x_m，y_m）が存在し得る。
【００４９】
ある実施形態では、テーブルn_iは、オフラインに構成されており、したがって、グラフの内周を最大にするように選択される。発見的には、以下でさらに説明するように、$n_i = c*i \mod T$（ただし、ｃはＴとの増分素数である）を設定することによって、望ましい結果がもたらされる。ある実施形態では、こうした技術によって、出力がバイトごとに入力と同じサイズであるという意味でロスのない結果がもたらされる。
【００５０】
置換：バッファサイズ、グラフ特性

グラフの内周は、ジェネレータによって出力される要素間の既知の関係について詳述するグラフＧの主な特性の１つである。線形攻撃を妨げるために重要な他のパラメータ（線形オペレータを用いた規則Ｅの更新に近似）は、最短の「単純」サイクルであり、例えば（図５に示される）対形成関数が厳密に２つ適用されたサイクルである。

【００５１】

$n_i = c * i \mod T$（ただし、ｃはＴとの増分素数である）と定義されるグラフについて考慮すると、可能な増分値を網羅的に探索することは比較的容易であり得る。以下の表１に、（ｎ＝８，１６，３２，１２８）について、内周および最小「単純」サイクルが最大化される例示的な増分値を列挙する。表１には、ｎ／２より小さいｃだけが示されている。

【００５２】

【表１】

バッファ長	増分値	内周	最小単純サイクル
T = 8	c = 3	6	4
16	3、5、7	6	6
32	7、9	8	10
64	19、27	8	12
128	15、17、47、49	8	18

表１．グラフＧの特性

【００５３】

追加のバッファ

図６に、記憶ユニットを繰り返し（帰納的に）回転することによって出力規則Ｈを強化するための例示的な方法６００を示す。図６に示すように、ある実施形態では、規則Ｈの出力を複雑にすることと引き換えに、遅延バッファおよび対形成関数を含む層を追加することが帰納的に適用される。また、対形成関数は、１サイクルの秘密の置換を使用してウォークスルーされる別のバッファを追加することによって単純化される。秘密の置換は、緩やかに変化し得る。ある実施形態では、方法６００によって、キーストリームジェネレータ（図１の１０２など）によって生成されたキーストリームが向上する。

【００５４】

可変遅延とともにランダム値で初期化される、遅延バッファＤが使用される。ある実施形態では、Ｓを１サイクルのランダム置換とする、更新関数遅延＝Ｓ［遅延］が使用される。図示するように、記憶ユニットを左にシフトする場合、以下の諸ステップが反復される。

【００５５】

１．Ｃ［ｉ］←出力規則Ｈによってもたらされる要素（６０２）。

２．対形成関数ｐ（Ａ［n_i］；Ｃ［ｉ］）の一部（左半分など）およびＤ［遅延］を提供する（６０４）。

３．対形成関数ｐの残りの部分（右半分など）をバッファＤ（Ｄ［遅延］）の遅延位置に挿入する（６０６）。

４．遅延の値を更新し、ｉ←ｉ＋１に設定する（６０８）。

５．ｉ＝Ｔであれば（６１０）、Ａ←Ｂ、Ｂ←Ｃ（６１２）、ｉ←０（６１４）。

【００５６】

もちろん、記憶ユニットを右にシフトする場合も、類似のステップが反復される（例えばステップ２で右半分を提供し、ステップ３で左半分を挿入し、ステップ５で記憶ユニットを右にシフトする）。さらに、ある実施形態では、最後の操作は、３つのバッファを指すポインタを回転することによって効率的に実施される。さらに、図２を参照して説明したように、方法６００の段階の実施に先立って、記憶ユニットＡおよびＢが（例えばランダム値または出力関数Ｈによって生成された値で）初期化される。

【００５７】
したがって、出力関数Ｈによって生成された要素（個々の文字またはビットなど）が格納される（６０２）。図２を参照して説明したように、要素を格納するために、バッファ、レジスタ、キャッシュまたは他のタイプのメモリなど、様々なタイプの装置または媒体が使用される。対形成関数ｐの結果の一部および遅延値（Ｄ［遅延］）（図３および４で示した記憶ユニットなどの少なくとも２つの対応する記憶ユニット内に格納された値など）が提供される（６０４）。対形成関数の残りの部分は、（遅延、例えばＤ［遅延］で索引付けされた）遅延バッファ内に挿入される（６０６）。記憶ユニットおよび遅延関数に索引付けするために使用されるインデックス、ならびに遅延バッファ（遅延）のインデックスが更新される（６０８）。

【００５８】
例えば更新されたインデックスを閾値と比較することによって判断されるが、所与の閾値に達しない場合（６１０）、方法６００は、段階６０２に戻って、出力規則Ｈによって生成された次の要素を格納する。そうでない場合、閾値に達すると（６１０によって判断される）、（例えば格納された値を左または右にシフトすることによって）記憶ユニットが回転される（６１２）。ついで、インデックスが（例えば０に）初期化され、方法６００は、段階６０２で再開して、出力規則Ｈによって生成された次の要素を格納する。方法６００は、所望の長さのキーストリームが生成されるまで実施される。

【００５９】
更新規則
図２および６を参照して説明するように、回転記憶ユニットを使用して、ストリーム暗号を強化することができる。ある実施形態では、比較的単純な更新が、図２および６の効率的な出力規則と組み合わせられる。こうした技術を使用して、ソフトウェア実装でも比較的効率的であり得る多種多様な新しい暗号を構成することができる。

【００６０】
ランダムウォーク、Ｔ関数、ＬＦＳＲ（ｌｉｎｅａｒ　ｆｅｅｄｂａｃｋ　ｓｈｉｆｔ　ｒｅｇｉｓｔｅｒ：線形フィードバックシフトレジスタ）、および断定された（ａｌｌｅｇｅｄ）ＲＣ４（Ｒｏｎ’ｓ　Ｃｏｄｅ　４－ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，ａｎｄ　Ａｄｌｅｍａｎ公開鍵暗号技術）のＲｏｎ　Ｒｉｖｅｓｔによる可変鍵サイズ暗号アルゴリズム）などのワードベースのストリーム暗号に基づく規則を含めて、いくつかの例示的な更新規則について以下で説明する。

【００６１】
エキスパンダグラフ（ｅｘｐａｎｄｅｒ　ｇｒａｐｈ）上のランダムウォーク
エキスパンダグラフは、（疑似）ランダム性の自然源であり、それには、エキストラクタ、デランダマイザなど、様々な応用がある。しかし、エキスパンダが暗号に応用される前に解決しなければならない問題が少しある。

【００６２】
ある実施形態では、基礎となるグラフは有向であると想定される。以下のウォークは、ケーリーグラフ上のウォークであると便宜上見なされる。ジュネレータＳ［１］，．．．，Ｓ［ｎ］を含むＧ上のケーリーグラフは一般に、形

【００６３】
【数５】
$(x, x \circ s[i])$

【００６４】
のノードおよびエッジとして、グループＧの要素を含む。

【００６５】
グラフが無向である場合、そのグラフがエキスパンダグラフを形成し、ランダムウォークが迅速に混在することが知られている。無向グラフを使用する際に、２つの重要な実用的な問題がある。まず、こうしたグラフでのウォークは、一定の数のステップで以前のノ

ードに戻る一定の確率を有する。この問題を解決する１つの方法は、有効な短期的特性を有する別のプロセスの状態に現在の状態（バイナリ列）を追加することであるが、これは、ストレージのサイズ（キャッシュサイズなど）を増加させ得る。グラフが有向である場合、この問題は対処されるが、伸張および迅速な混在の特性を確保する問題に依然として対処する必要があり得る。グラフにオイラーの向きが与えられる場合、伸張を確実にすることができる。さらに、グラフが大きい有向グラフであれば、短期の戻りの確率は、最小限に抑えられ得る。

【００６６】

効率的な実施を可能にするいくつかの例示的なグラフには以下のものがある。

【００６７】

加法型ウォーク（ａｄｄｉｔｉｖｅ　ｗａｌｋ）。ｘ：＝ｘ＋ｓ［ｉ］。本式でＳは、法2^nの下の加法群内のランダム要素のテーブルである。

【００６８】

乗法型ウォーク（ｍｕｌｔｉｐｌｅ　ｗａｌｋ）。

【００６９】

【数６】

$$x := x \bullet s[i] \bmod 2^n$$

【００７０】

本式でＳは、法（モジュロ，ｍｏｄｕｌｏ）2^nの下の乗法群内のランダム要素のテーブルである。

【００７１】

ガバー－ガリル（Ｇａｂｂｅｒ－Ｇａｌｉｌ）型ウォーク。このグラフは、シフトおよび加算を用いて実施される更新規則Ｅを有する。無向グラフと同様に、これは、エキスパンダであることが明らかになっている。

【００７２】

ラマヌジャン型ウォーク。このグラフは、ＬＰＳ（Ｌｕｂｏｔｚｋｙ，Ｐｈｉｌｌｉｐｓ，ａｎｄ　Ｓａｒｎａｋ）によって定義されている。このグラフは、効率的に実施するのが比較的難しい。それは、無向グラフと同様に、優れたエキスパンダであり、また大きい内周（すなわちグラフのサイズの対数）を有することも分かっている。ある実施形態では、このグラフは、有向グラフとして使用される。

【００７３】

置換型ウォーク（ｐｅｒｍｕｌａｔｉｏｎ　ｗａｌｋ）。このグラフはS_nであり、更新規則Ｅは２つのランダム位置をスワップする。このウォークは、迅速に混在することが知られている。これは、断定されたＲＣ４のモデルとして使用される。

【００７４】

動的ジェネレータを用いたランダムウォーク。これは、ケーリーグラフのジェネレータの更新規則Ｅを提示する。

【００７５】

状態更新のための反復Ｔ関数

可逆性の写像$\{0, 1\}^n \rightarrow \{0, 1\}^n$（Ｔ関数と称される）のクラスによって、基本のレジスタ操作

【００７６】

【数７】

$$\left(\vee, \wedge, \oplus, *, +, -, x \mapsto \bar{x}, x \mapsto -x, [] << \text{など}\right)$$

【００７７】

を用いて非線形性を取り入れることが可能である。ある実施形態では、一部には比較的より高速なソフトウェアソリューションのために、Ｔ関数を使用して、更新関数を提供する。

【００７８】
こうした関数の一例は、ｆ（ｘ）＝ｘ＋（ｘ^{2}∨５）ｍｏｄ２^{n}であり、ただし、列ｘ$_{i+1}$＝ｆ（ｘ$_{i}$）は１サイクルの領域全体に渡る。ある実施形態では、それぞれの反復に、３つのサイクルだけが必要である。ｎ＝６４を選択し、ｘ$_{i}$の上位半分（すなわちＨ（ｘ$_{i}$）＝ＭＳＢ$_{32}$（ｘ$_{i}$））を出力することによって、有意水準（ｓｉｇｎｉｆｉｃａｎｔ　ｌｅｖｅｌ）α＝０．０１を有するＡＥＳ（ａｄｖａｎｃｅｄ　ｅｎｃｒｙｐｔｉｏｎ　ｓｅｒｖｉｃｅ：高度暗号サービス）のための統計的なテストスィートにパスする疑似乱数列がもたらされる。最も知られている解読は、反復出力の構造を使用することに依存しており、またｃを定数として、時間２^{cn}を一般に要する。したがって、その構造は、こうした関数の特性を証明するのに重要であり、構造を多少変更することによって、その特性が破壊される。こうした関数によって、一定の制約付きで、そのパラメータの一部をランダムに選択することができる。本明細書で説明する実施形態は、最小限のオーバヘッドでこうした攻撃に耐え、またストリーム暗号の基礎となる鍵の長さを長くすることが想定されている。

【００７９】
状態更新のためのＬＦＳＲ規則およびこうしたジェネレータの組合せ
比較的多数のストリーム暗号が線形フィードバックシフトレジスタ（ＬＦＳＲ：ｌｉｎｅａｒ－ｆｅｅｄｂａｃｋ　ｓｈｉｆｔ　ｒｅｇｉｓｔｅｒ）に基づいている。その一部の理由には、それがハードウェア実装に適しており、比較的大きい期間の列を生成し、比較的有効な統計的特性を有する列を生成し、またその構造のために、代数的技術を使用して容易に解析されることがある。また後者は、ＬＦＳＲの正確な出力列を隠すことを必要とする。

【００８０】
収縮（ｓｈｒｉｎｋｉｎｇ）ジェネレータ、クロックベースのジェネレータ、アルゴリズムＭ（すなわちマクローリン－マーサグリアアルゴリズム）に基づくジェネレータおよび／またはアルゴリズムＢ（すなわちベイズ－ダーハムトリック）などの様々なやり方で出力を組み合わせる、ＬＦＳＲの様々な構成が使用される。ＬＦＳＲに関するさらなる情報および他の暗号の基本については、非特許文献１に記載のテキストを参照されたい。

【００８１】
Ｓ$_{256}$上のワードベースのストリーム暗号
ワードベースのストリーム暗号は一般に、例えば２５６要素のテーブルとしてＳ$_{256}$の要素のコンパクト表現を使用して、バイトレベルで機能する。

【００８２】
【数８】
$S_{2^{32}}$

【００８３】
に拡張するには、今日の技術による非実用的なテーブルサイズを伴う。代替として、テーブルコーディングδ∈Ｓ$_{256}$は、法２５６の下のテーブルが依然としてδであるように２４ランダムビット追加して、テーブルの各エントリを拡張することによって、ワード配列に拡張することができる。したがって、テーブルのエントリは、関数ｆ$_{a,b}$＝ａｘ＋ｂ（ただし、要素ａ，ｂ自体は

【００８４】
【数９】
$(Z_{2^{32}},+)$および$(Z_{2^{32}},*)$

【００８５】
上のランダムウォークを使用して更新されている）を使用して最下位バイトを保持しながら更新されている。

【００８６】

ハードウェア実装

図７に、本明細書で説明する技術を実施するために使用される一般的なコンピュータ環境７００を示す。例えば、コンピュータ環境７００を使用して、上記の図面を参照して説明したタスクの実施に関連する命令を実行することができる。コンピュータ環境７００は、コンピューティング環境の一例にすぎず、コンピュータおよびネットワークアーキテクチャの使用または機能の範囲に関する限定を示唆することは意図されていない。コンピュータ環境７００は、例示的なコンピュータ環境７００内に示す構成要素のいずれか１つまたはその組合せに関する依存関係または要求を有すると解釈されるべきでない。

【００８７】

コンピュータ環境７００は、コンピュータ７０２の形の汎用コンピューティング装置を含む。コンピュータ７０２の構成要素は、それだけに限らないが、１つまたは複数のプロセッサまたは処理装置７０４（任意選択で暗号プロセッサまたはコプロセッサを含む）、システムメモリ７０６、およびプロセッサ７０４を含めて様々なシステム構成要素をシステムメモリ７０６に結合するシステムバス７０８を含み得る。

【００８８】

システムバス７０８は、メモリバスまたはメモリコントローラ、周辺バス、アクセラレイテッドグラフィックポート、および様々なバスアーキテクチャのいずれかを用いたプロセッサまたはローカルバスを含めて、複数タイプのバス構造のいずれかの１つまたは複数を表す。例を挙げると、こうしたアーキテクチャは、業界標準アーキテクチャ（ＩＳＡ：Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、マイクロチャネルアーキテクチャー（ＭＣＡ：Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、拡張ＩＳＡ（ＥＩＳＡ：Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ビデオ電子規格協会（ＶＥＳＡ：Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、およびメザニンバスとも呼ばれる周辺コンポーネント相互接続（ＰＣＩ：Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔｓ）バスが含まれ得る。

【００８９】

コンピュータ７０２は一般に、様々なコンピュータ読取り可能媒体を含む。こうした媒体は、コンピュータ７０２からアクセスすることができ、また揮発性と不揮発性、取出し可能と取出し不可能の両方の媒体を含む使用可能な任意の媒体であり得る。

【００９０】

システムメモリ７０６は、ランダムアクセスメモリ（ＲＡＭ）７１０などの揮発性メモリおよび／または読出し専用メモリ（ＲＯＭ）７１２などの不揮発性メモリの形のコンピュータ読取り可能媒体を含む。起動時などにコンピュータ７０２内の要素間で情報を転送する助けとなる基本ルーチンを含む基本入出力システム（ＢＩＯＳ）７１４は、ＲＯＭ７１２に格納される。ＲＡＭ７１０は一般に、処理装置７０４によって直接にアクセス可能であり、および／またはそれによる操作を現在受けているデータおよび／またはプログラムモジュールを含む。

【００９１】

コンピュータ７０２は、他の取出し可能／取出し不可能、揮発性／不揮発性のコンピュータ記憶媒体をも含み得る。例示するために、図７に、取出し不可能な不揮発性の磁気媒体（図示せず）から読み出し、またそこに書き込むためのハードディスクドライブ７１６、取出し可能な不揮発性の磁気ディスク７２０（「フロッピー（登録商標）ディスク」など）から読み出し、またそこに書き込むための磁気ディスクドライブ７１８、およびＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭまたは他の光媒体などの取出し可能な不揮発性の光ディスク７２４に対して読出しおよび／または書込みを行うための光ディスクドライブ７２２を示す。ハードディスクドライブ７１６、磁気ディスクドライブ７１８および光ディスクドライブ７２２はそれぞれ、１つまたは複数のデータメディアインターフェース７２６によってシステムバス７０８に接続される。代わりに、ハードディスクドライブ７１６、磁気ディスクドライブ７１８および光ディスクドライブ７２２は、１つまたは複数のインターフェ

ース（図示せず）によってシステムバス７０８に接続される。

【００９２】

ディスクドライブおよびその関連のコンピュータ記憶媒体によって、コンピュータ読取り可能命令、データ構造体、プログラムモジュール、およびコンピュータ７０２のその他のデータの不揮発性の記憶域がもたらされる。この例には、ハードディスク７１６、取出し可能磁気ディスク７２０、および取出し可能光ディスク７２４が示されているが、磁気カセットまたは他の磁気記憶装置、フラッシュメモリカード、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）また他の光ストレージ、ランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、電気的消去可能プログラマブル読出し専用メモリ（ＥＥＰＲＯＭ）など、コンピュータによってアクセス可能なデータを格納することができる他のタイプのコンピュータ読取り可能媒体を使用して、例示的なコンピューティングシステムおよび環境を実施することもできることを理解されたい。

【００９３】

例えば、オペレーティングシステム７２６、１つまたは複数のアプリケーションプログラム７２８、他のプログラムモジュール７３０およびプログラムデータ７３２を含めて、任意の数のプログラムモジュールが、ハードディスク７１６、磁気ディスク７２０、光ディスク７２４、ＲＯＭ７１２および／またはＲＡＭ７１０に格納される。こうしたオペレーティングシステム７２６、１つまたは複数のアプリケーションプログラム７２８、他のプログラムモジュール７３０およびプログラムデータ７３２のそれぞれ（またはその組合せ）によって、分散ファイルシステムをサポートする常駐の構成要素のすべてまたは一部を実施することができる。

【００９４】

ユーザは、キーボード７３４、ポインティング装置７３６（「マウス」）など）の入力装置を用いて、コンピュータ７０２にコマンドおよび情報を入力することができる。他の入力装置７３８（具体的には図示せず）は、マイク、ジョイスティック、ゲームパッド、パラボラアンテナ、シリアルポート、スキャナおよび／またはその同類物などを含み得る。これらのおよび他の入力装置は、システムバス７０８に結合される入出力インターフェース７４０を介して処理装置７０４に接続されるが、パラレルポート、ゲームポートまたはユニバーサルシリアルバス（ＵＳＢ）など、他のインターフェースおよびバス構造によって接続されることもできる。

【００９５】

モニタ７４２または他のタイプの表示装置もまた、ビデオアダプタ７４４などのインターフェースを介してシステムバス７０８に接続される。他の出力周辺装置は、モニタ７４２に加え、入出力インターフェース７４０を介してコンピュータ７０２に接続されるスピーカ（図示せず）およびプリンタ７４６などの構成要素を含み得る。

【００９６】

コンピュータ７０２は、リモートコンピューティング装置７４８などの１つまたは複数のリモートコンピュータへの論理接続を使用して、ネットワーク化された環境で動作することができる。例を挙げると、リモートコンピューティング装置７４８は、パーソナルコンピュータ、ポータブルコンピュータ、サーバ、ルータ、ネットワークコンピュータ、ピアデバイスまたは他の通常のネットワークノード、ゲームコンソールなどとすることができる。リモートコンピューティング装置７４８は、本明細書でコンピュータ７０２に関して説明した要素および特徴の多くまたはすべてを含み得るポータブルコンピュータとして図示されている。

【００９７】

コンピュータ７０２とリモートコンピューティング装置７４８の間の論理接続は、ローカルエリアネットワーク（ＬＡＮ）７５０、および一般的な広域エリアネットワーク（ＷＡＮ）７５２として示されている。こうしたネットワーキング環境は、オフィス、企業規模のコンピュータネットワーク、イントラネットおよびインターネットでは一般的である。

【００９８】
ＬＡＮネットワーキング環境内で実施される場合、コンピュータ７０２は、ネットワークインターフェースまたはアダプタ７５４を介してローカルネットワーク７５０に接続される。ＷＡＮネットワーキング環境内で実施される場合、コンピュータ７０２は一般に、モデム７５６、または広域ネットワーク７５２を介して通信を確立する他の手段を含む。内部にあることも、外部にあることもあるモデム７５６は、入出力インターフェース７４０または他の適切な機構を介してシステムバス７０８に接続される。図示されるネットワーク接続は例であり、コンピュータ７０２と７４８間の通信リンクを確立する他の手段が使用されることを理解されたい。

【００９９】
コンピューティング環境７００によって示した環境などのネットワーク化された環境では、コンピュータ７０２に関して示したプログラムモジュールまたはその一部は、リモートメモリ記憶装置内に格納される。例を挙げると、リモートアプリケーションプログラム７５８は、リモートコンピュータ７４８のメモリ装置内に常駐する。図示するため、本明細書では、アプリケーションプログラム、およびオペレーティングシステムなどの他の実行可能プログラム構成要素が別個のブロックとして示されているが、こうしたプログラムおよび構成要素は、様々なときにコンピューティング装置７０２のそれぞれ異なるストレージ構成要素内に常駐し、コンピュータのデータプロセッサによって実行されることが理解されよう。

【０１００】
本明細書では、様々なモジュールおよび技術について、１つまたは複数のコンピュータまたは他の装置によって実行されるプログラムモジュールなどのコンピュータ実行可能命令の一般的な文脈で説明することができる。プログラムモジュールは一般に、特定のタスクを実施し、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造体などを含む。プログラムモジュールの機能は一般に、様々な実施形態で所望されるように組み合わせられ、または分散される。

【０１０１】
こうしたモジュールおよび技術の実施形態は、何らかの形態のコンピュータ読取り可能媒体内に格納されても、それ全体に渡って送信されてもよい。コンピュータ読取り可能媒体は、コンピュータによってアクセスすることができる使用可能な任意の媒体であり得る。限定のためでなく、例を挙げると、コンピュータ読取り可能媒体には、「コンピュータ記憶媒体」および「通信媒体」が含まれ得る。

【０１０２】
「コンピュータ記憶媒体」は、コンピュータ読取り可能命令、データ構造体、プログラムモジュールまたは他のデータなどの情報を格納するための任意の方法または技術で実施された揮発性と不揮発性、取出し可能と取出し不可能媒体を含む。コンピュータ記憶媒体には、それだけに限らないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）または他の光ストレージ、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶装置、あるいは所望の情報を格納するために使用することができ、またコンピュータによってアクセスすることができる他の任意の媒体が含まれる。

【０１０３】
「通信媒体」は一般に、コンピュータ読取り可能命令、データ構造体、プログラムモジュール、または搬送波や他のトランスポート機構などの変調されたデータ信号の形の他のデータを含む。通信媒体は、任意の情報送達媒体をも含む。用語「変調されたデータ信号」は、信号に情報を符号化するようにその特性の１つまたは複数が設定されまたは変更された信号を意味する。限定のためではなく、例を挙げると、通信媒体には、有線ネットワークや直接有線接続などの有線媒体、ならびに音響、無線周波数（ＲＦ）、赤外線（ＩＲ）、ワイヤレスフィデリティ（ＩＥＥＥ８０２．１１ｂ無線ネットワーキング）（Ｗｉ－Ｆｉ：ｗｉｒｅｌｅｓｓ　ｆｉｄｅｌｉｔｙ）、セルラ、Ｂｌｕｅｔｏｏｔｈ対応型およ

び他の無線媒体などの無線媒体が含まれる。上記内容のいずれかの組合せもまた、コンピュータ読取り可能媒体の範囲内に含まれる。

【０１０４】

結論

本発明について構造上の特徴および／または方法論的行為に特有の言語で説明したが、添付の特許請求の範囲中に定められる本発明は、説明した具体的な特徴または行為に必ずしも限定されないことを理解されたい。そうではなく、具体的な特徴または行為は、特許請求の範囲に記載された発明を実施する例示的な形として開示されている。

【図面の簡単な説明】

【０１０５】

【図１】例示的なストリーム暗号システムを示す図である。

【図２】回転記憶ユニットを使用することによって出力規則Ｈを強化するための例示的な方法を示す図である。

【図３】回転記憶ユニットの例示的な対形成を示す図である。

【図４】回転記憶ユニットの対形成に対応する例示的な無向グラフを示す図である。

【図５】回転記憶ユニットに対応する例示的な最短「単純」サイクルグラフを示す図である。

【図６】記憶ユニットを帰納的に回転することによって出力規則Ｈを強化するための例示的な方法を示す図である。

【図７】本明細書で説明する技術を実施するために使用される一般的なコンピュータ環境７００の図である。

【符号の説明】

【０１０６】

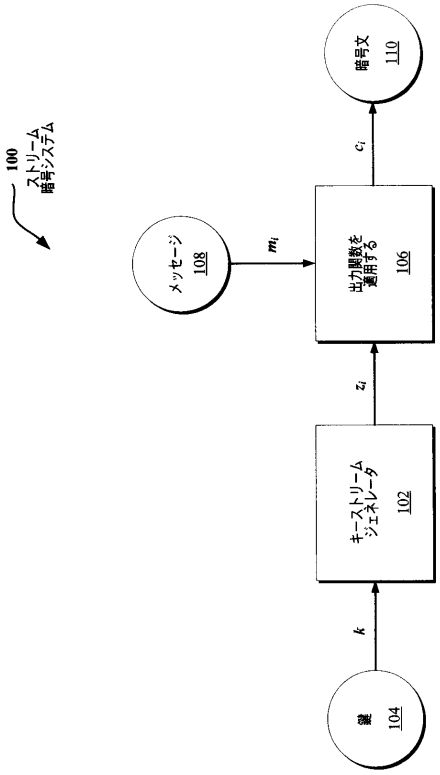
１０２　キーストリームジェネレータ

１０４　鍵

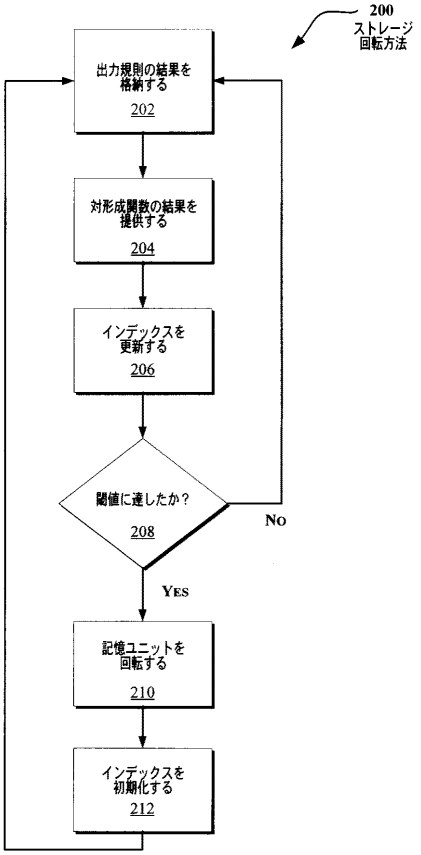
１０８　メッセージ

１１０　暗号文

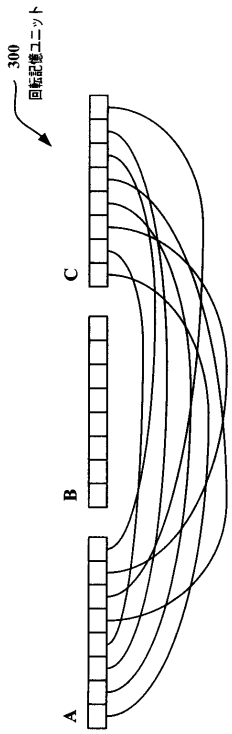
【図１】


100
ストリーム
暗号システム
メッセージ
108
m_i
出力関数を
適用する
106
c_i
暗号文
110
z_i
キーストリーム
ジェネレータ
102
k
鍵
104

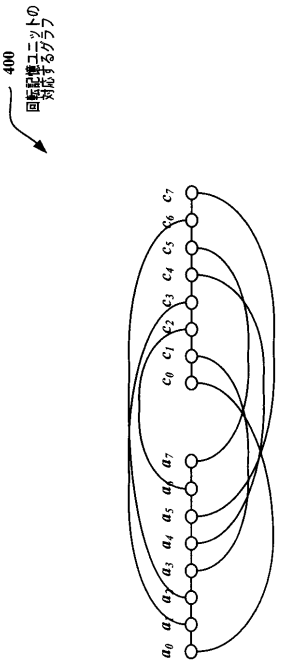
【図２】


200
ストレージ
回転方法
出力規則の結果を
格納する
202
対形成関数の結果を
提供する
204
インデックスを
更新する
206
閾値に達したか？
208
No
Yes
記憶ユニットを
回転する
210
インデックスを
初期化する
212

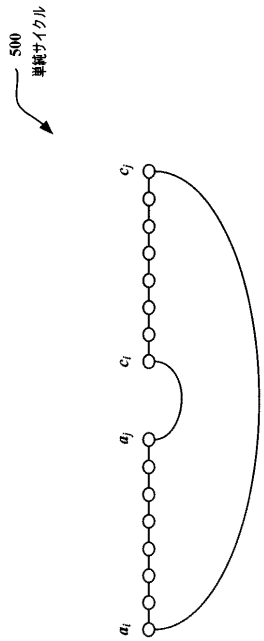
【図３】


300
回転記憶ユニット
A
B
C

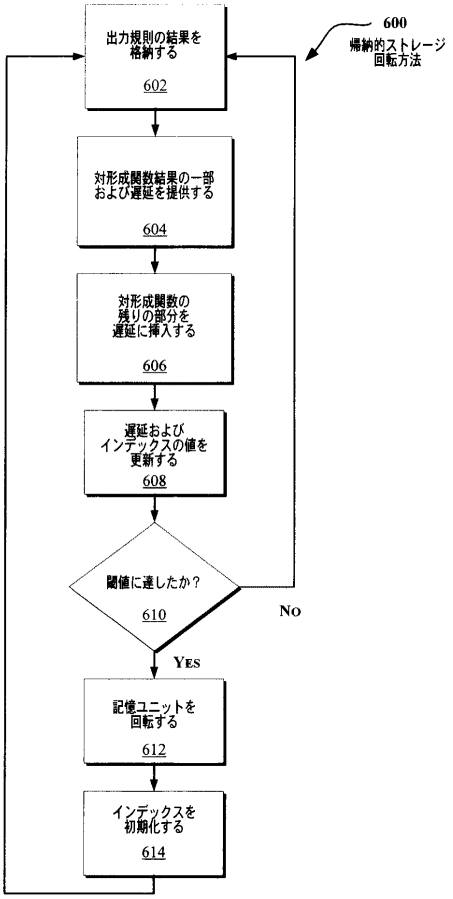
【図４】


400
回転記憶ユニットの
対応するグラフ
c_7
c_6
c_5
c_4
c_3
c_2
c_1
c_0
a_7
a_6
a_5
a_4
a_3
a_2
a_1
a_0

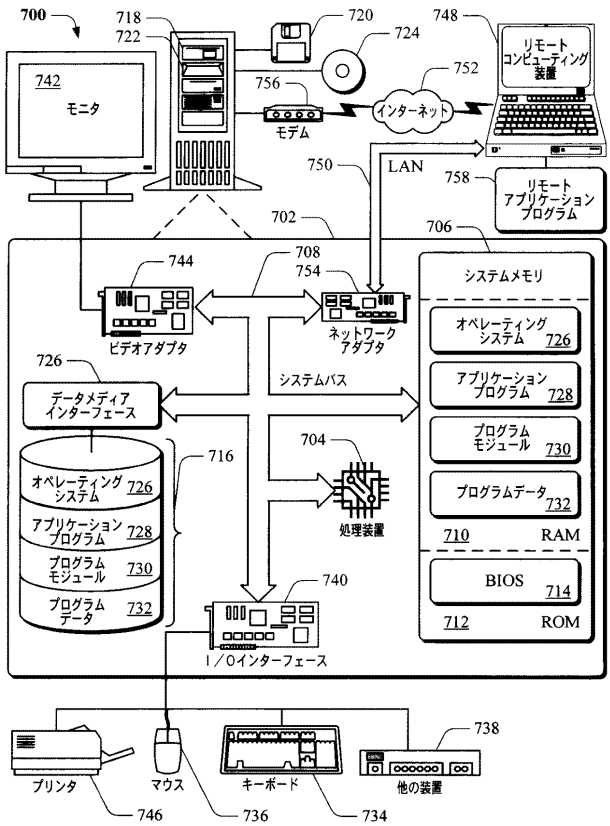
【図５】


500
単純サイクル
c_j
c_i
a_j
a_i

【図６】


600
帰納的ストレージ回転方法
出力規則の結果を格納する
602
対形成関数結果の一部および遅延を提供する
604
対形成関数の残りの部分を遅延に挿入する
606
遅延およびインデックスの値を更新する
608
閾値に達したか？
610
No
Yes
記憶ユニットを回転する
612
インデックスを初期化する
614

【図７】


700
718
722
720
724
748
752
742
モニタ
756
モデム
インターネット
リモートコンピューティング装置
750
LAN
758
リモートアプリケーションプログラム
702
706
744
708
754
システムメモリ
ビデオアダプタ
ネットワークアダプタ
オペレーティングシステム 726
726
システムバス
データメディアインターフェース
アプリケーションプログラム 728
プログラムモジュール 730
704
716
プログラムデータ 732
処理装置
710
RAM
BIOS 714
740
712
ROM
I／Oインターフェース
738
プリンタ
マウス
キーボード
他の装置
746
736
734

フロントページの続き

(72)発明者　ラマラスナム　ベンカテサン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

Ｆターム(参考) 5J104 AA01　AA12　JA04　NA08　NA27　PA14