

(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2007-60191

(P2007-60191A)

(43) 公開日 平成19年3月8日(2007.3.8)

(51) Int. Cl. F I テーマコード (参考)
 H04L 9/26 (2006.01) H04L 9/00 659 5J104

審査請求 未請求 請求項の数 2 O L (全 9 頁)

(21) 出願番号	特願2005-242051 (P2005-242051)	(71) 出願人 000208891
(22) 出願日	平成17年8月24日 (2005.8.24)	KDDI株式会社 東京都新宿区西新宿二丁目3番2号
		(74) 代理人 100101465 弁理士 青山 正和
		(74) 代理人 100064908 弁理士 志賀 正武
		(74) 代理人 100089037 弁理士 渡邊 隆
		(72) 発明者 清本 晋作 埼玉県上福岡市大原2丁目1番15号 株式会社KDDI研究所内
		(72) 発明者 田中 俊昭 埼玉県上福岡市大原2丁目1番15号 株式会社KDDI研究所内

最終頁に続く

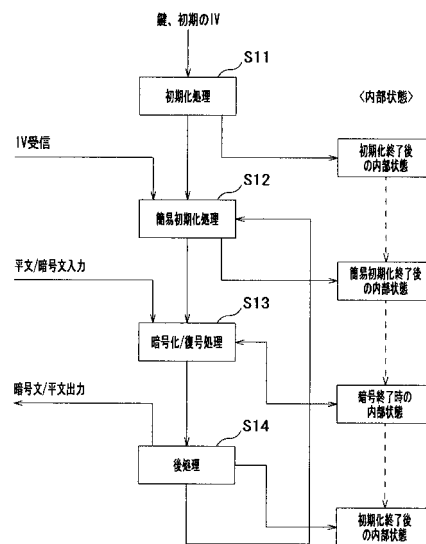
(54) 【発明の名称】 ストリーム暗号方法および装置

(57) 【要約】

【課題】 頻繁に初期値が更新される環境でストリーム暗号を使用する場合にも、安全、高速に初期化処理を実現する。

【解決手段】 通常の初期化処理 (S11) が終了した内部状態と、暗号化処理 (S13) 時の内部状態とをそれぞれ独立して管理する。このために、暗号化処理 (S13) 時に簡易初期化処理 (S12) を実行し、内部状態を更新した後に暗号化処理 (S13) を行い、暗号化処理 (S13) 終了後にその内部状態を消去して通常の初期化処理終了時の内部状態を復元する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

線形フィードバックレジスタを備え、前記線形フィードバックレジスタの出力に非線形関数演算を施してキーストリームを生成し、入力される平文を前記キーストリームにより暗号化するストリーム暗号方法であって、

外部から前記鍵情報と初期値とを所定の周期で受信し、所定のアルゴリズムに従い決定されるストリーム暗号の内部状態を前記線形フィードバックレジスタに入力して初期攪拌を行うと共に、前記初期攪拌終了後の内部状態を内部状態メモリに保存する初期化処理ステップと、

前記初期化処理ステップにおける周期よりも短い周期で到来する初期値を受信し、前記初期値と前記内部状態メモリに保存された前記初期攪拌終了後の内部状態とを演算して前記内部状態メモリに保持する簡易初期化処理ステップと、

前記内部状態メモリに保持された内部状態を使用してキーストリームを生成し、前記キーストリームと外部から入力される平文とを演算して暗号化を行い、前記内部状態を動的に更新する暗号化処理ステップと、

前記暗号化が終了し、もしくは前記初期値の入力があった場合、前記内部状態メモリに保持された内部状態を消去し、前記内部メモリに保存されている初期攪拌終了後の内部状態を復元して前記簡易初期化処理ステップ以降の処理ステップを繰り返し実行する後処理ステップと、

を有することを特徴とするストリーム暗号方法。

【請求項 2】

線形フィードバックレジスタを備え、前記線形フィードバックレジスタの出力に非線形関数演算を施してキーストリームを生成し、入力される平文を前記キーストリームにより暗号化するストリーム暗号装置であって、

外部から鍵情報と初期値とを所定の周期で受信し、所定のアルゴリズムに従い決定されるストリーム暗号の内部状態を前記線形フィードバックシフトレジスタに入力して初期攪拌を行うと共に、前記初期攪拌終了後の内部状態を内部状態メモリに保存する第 1 の内部状態生成部と、

前記所定の周期よりも短い周期で到来する初期値を受信し、前記初期値と前記内部状態メモリに保存された前記初期攪拌終了後の内部状態とを演算し、その結果を前記内部状態メモリに保持する第 2 の内部状態生成部と、

前記内部状態メモリに保持された内部状態を使用してキーストリームを生成し、前記キーストリームと外部から入力される平文とを演算して暗号化を行い、前記内部状態を動的に更新する暗号化処理部と、

前記暗号化処理部による暗号化が終了し、もしくは前記初期値の入力があった場合、前記内部状態メモリに保持された内部状態を消去し、前記内部状態メモリに保存されている初期攪拌終了後の内部状態を復元する内部状態復元部と、

を備えたことを特徴とするストリーム暗号装置。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、線形フィードバックレジスタを備え、当該線形フィードバックレジスタの出力に非線形関数演算を施してキーストリームを生成し、当該キーストリームと平文とを演算して暗号化する、ストリーム暗号方法および装置に関する。

【背景技術】**【0002】**

近年、コンピュータを利用した様々なサービスが提供されている。多くのサービスにおいては、通信の秘匿を実現するために、暗号が利用される。暗号化方式として、最も一般的なものは、一つの鍵で暗号化・復号化を行う共通鍵暗号化方式であるが、この共通暗号

10

20

30

40

50

化方式は、ブロック暗号方式とストリーム暗号方式の2つに大別される。

前者は、最も一般的に用いられている方式であるが、後者の方が処理速度に優れるため、近年注目を集めつつある。

【0003】

上記したストリーム暗号を生成するための方法および装置の一例が以下の特許文献に開示されている。

【特許文献1】特表2002-536912号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

ところで、上記したストリーム暗号には、初期化処理に時間を要するといった問題がある。ここでいう「初期化処理」とは、内蔵のキースケジューアルゴリズムによるストリーム暗号の内部状態（擬似乱数）の決定と、この内部状態を線形フィードバックレジスタ（LFSR）に入力した後、複数回空廻しを行う初期攪拌処理をいう。

【0005】

上記した初期化処理は、外部から入力される初期値（初期ベクトルIV）が変更になる毎に最初から実行し直す必要があり、特に、放送データの暗号化等、途中から視聴参加するユーザのために回避できない問題であり、システム性能上無視できないものであった。

【0006】

本発明は上記事情に基づいてなされたものであり、頻繁に初期値が更新される環境でストリーム暗号を使用する場合にも、安全、高速に初期化処理を実現することのできる、ストリーム暗号方法および装置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】

【0007】

上記した課題を解決するために本発明は、線形フィードバックレジスタを備え、前記線形フィードバックレジスタの出力に非線形関数演算を施してキーストリームを生成し、入力される平文を前記キーストリームにより暗号化するストリーム暗号方法であって、外部から前記鍵情報と初期値とを所定の周期で受信し、所定のアルゴリズムに従い決定されるストリーム暗号の内部状態を前記線形フィードバックレジスタに入力して初期攪拌を行うと共に、前記初期攪拌終了後の内部状態を内部状態メモリに保存する初期化処理ステップと、前記初期化処理ステップにおける周期よりも短い周期で到来する初期値を受信し、前記初期値と前記状態メモリに保存された前記初期攪拌終了後の内部状態とを演算し、その結果を前記内部状態メモリに保持する簡易初期化処理ステップと、前記内部状態メモリに保持された内部状態を使用してキーストリームを生成し、前記キーストリームと外部から入力される平文とを演算して暗号化を行い、前記内部状態を動的に更新する暗号化処理ステップと、前記暗号化処理部による暗号化が終了、もしくは前記初期値の入力があった場合、前記内部状態メモリに保持された内部状態を消去し、前記内部メモリに保存されている初期攪拌終了後の内部状態に基づき、前記簡易初期化処理ステップ以降の処理ステップを繰り返し実行する後処理ステップと、を有することを特徴とする。

【0008】

また、本発明は、線形フィードバックレジスタを備え、前記線形フィードバックレジスタの出力に非線形関数演算を施してキーストリームを生成し、当該キーストリームと平文とを演算して暗号化するストリーム暗号装置であって、外部から鍵情報と初期値とを所定の周期で受信し、所定のアルゴリズムに従い決定されるストリーム暗号の内部状態を前記線形フィードバックシフトレジスタに入力して初期攪拌を行い、前記初期攪拌終了後の内部状態を内部状態メモリに保存する第1の内部状態生成部と、前記所定の周期よりも短い周期で到来する初期値を受信し、前記初期値と前記状態メモリに保存された前記初期攪拌終了後の内部状態とを演算し、その結果を前記内部状態メモリに保持する第2の内部状態生成部と、前記内部状態メモリに保持された内部状態を使用してキーストリームを生成し、前記キーストリームと外部から入力される平文とを演算して暗号化を行い、前記内部状

10

20

30

40

50

態を動的に更新する暗号化処理部と、前記暗号化処理部による暗号化が終了、もしくは前記初期値の入力があった場合、前記内部状態メモリに保持された内部状態を消去し、前記内部状態メモリに保存されている初期攪拌終了後の内部状態を復元する内部状態復元部と、を備えたことを特徴とする。

【発明の効果】

【0009】

本発明によれば、通常の初期化処理が終了した内部状態と、暗号化処理時の内部状態を独立に管理し、暗号化処理時、本発明により付加される簡易初期化処理を実行して内部状態を更新した後に暗号化処理を行い、暗号化処理終了後にその内部状態を消去して通常の初期化終了時の内部状態を復元することにより、頻繁に初期値が更新される環境にあっても、高速、かつ安全なストリーム暗号を実現することができる。

10

【0010】

本発明は、一定周期で初期値を送信し、途中から受信したユーザもストリーム暗号を用いて復元を行う放送データの暗号化の初期化処理に用いて特に顕著な効果が得られる。

【発明を実施するための最良の形態】

【0011】

図1は、本発明の実施形態にかかわるストリーム暗号方法の手順を示すフローチャートである。

以下、図1に示すフローチャートを参照しながら本発明の実施形態にかかわるストリーム暗号方法の処理手順のそれぞれについて詳細に説明する。

20

【0012】

まず、通常の初期化処理(S11)から説明する。本発明の実施形態にかかわるストリーム暗号装置は、まず、外部から秘密鍵(IK: Initial Key)と、初期値(IV: Initial Value)を受信し、内蔵のキースケジュールアルゴリズムを実行して決定される内部状態を、後述する線形フィードバックレジスタ(LFSR-A、LFSR-B)に供給する。

【0013】

続いて線形フィードバックレジスタ(LFSR-A、LFSR-B)は、複数回空回しを行うことで比較的時間を要する初期攪拌処理を行う。そして、初期攪拌処理終了後の内部状態を後述する内部状態メモリに保存する。

30

【0014】

次に、本発明により付加される簡易初期化処理(S12)が実行される。この簡易初期化処理においては、図2にその詳細がフローチャートとして示されるように、まず、一定周期で初期値(IV)を受信する(S121、S122)。ここで初期値(IV)は、初期化処理時における周期よりは短く頻繁に送信されるものとし、内部状態と同じ300~400ビット程度の長さを持つものとする。

【0015】

そして、ここで受信した初期値(IV)を、図1に示す初期化処理(S11)における初期攪拌終了後の内部状態と、例えばXOR(排他的論理和)演算することにより足し合わせ、内部状態を更新する(S123)。このXOR演算の結果、生成される内部状態は、暗号化/復号化処理用として内部状態メモリに一時保持される(S124)。なお、ここでは、初期化処理時のような時間の要する攪拌処理は行なわれない。

40

【0016】

説明を図1に戻して説明を続ける。上記した簡易初期化処理(S12)に続いて暗号化/復号化処理(S13)が実行される。

暗号化/復号化処理(S13)では、平文もしくは暗号文が入力され、上記した簡易初期化処理(S12)時に更新された内部状態を使ってキーストリームを生成し、平文(暗号文)と、生成されたキーストリームとをXOR演算することにより暗号化(復号化)を行う。ここで、内部状態は、暗号化(復号化)処理中、動的に更新され、都度内部状態メモリに反映されるものとする。

50

【0017】

最後に、後処理（S14）について説明する。後処理は、暗号化（復号化）処理終了時、あるいは初期値（IV）の変更があったときに起動され、内部状態メモリに保持されている内部状態を消去し、先に保存しておいた初期攪拌終了後の内部状態を復元する処理を実行する。そして、S12の処理に戻り、簡易初期化処理以降の処理を、暗号化（復号化）処理終了、あるいは初期値（IV）の変更がある迄繰り返す。

【0018】

以上説明のように、本発明のストリーム暗号方法は、通常の初期化処理（S11）が終了した内部状態と、暗号化処理（S13）時の内部状態とをそれぞれ独立して管理することを特徴とするものである。このために、暗号化処理（S13）時に簡易初期化処理（S12）を実行し、内部状態を更新した後に暗号化処理（S13）を行い、この暗号化処理終了後にその内部状態を消去して通常の初期化処理終了時の内部状態を復元する各手順を実行する。

10

【0019】

このことにより、頻繁に初期値が更新される環境にあっても、高速なストリーム暗号を実現することができ、また、初期値（IV）に完全な乱数を用いることで安全性も実現できるものである。

【0020】

図3は、本発明の実施形態にかかわるストリーム暗号装置の内部構成を示すブロック図である。

20

本発明の実施形態にかかわるストリーム暗号装置は、内部状態生成部1と、LFSR-A(2)と、クロックコントローラ3と、LFSR-B(4)と、内部状態メモリ5と、非線形関数発生器6と、内部状態復元部7とで構成される。

【0021】

内部状態生成部1は、第1と第2の内部状態生成部から成る。第1の内部状態生成部は、外部から秘密鍵（IK）と初期値（IV）とを所定の周期で受信し、内蔵のキースケジューアルゴリズムを実行して決定される内部状態を、ストリーム暗号の内部状態（擬似乱数）発生用に使用される、LFSR-A(2)とLFSR-B(4)のそれぞれに入力して初期攪拌を行い、当該初期攪拌終了後の内部状態を内部状態メモリ5に保存する。

【0022】

また、第2の内部状態生成部は、上記より短い周期で到来する初期値（IV）を受信し、当該初期値と内部状態メモリ5に保存された初期攪拌終了後の内部状態とを演算し、その結果を内部状態メモリ5に保持する。

30

【0023】

なお、LFSR-B(4)により生成されるキーストリームは、キーストリームを生成する非線形関数発生器6の入力として供給されている。ここで、非線形関数発生器6は、入力されたキーストリームと、内部状態メモリ5に保持された内部状態とにより、ある非線形関数演算を実行して新たなキーストリームを生成する。

【0024】

一方、非線形関数発生器6の出力は内部状態メモリ5にも供給されており、更新された内部状態メモリ5の出力は非線形関数発生器6にフィードバック入力される。また、LFSR-A(2)は、クロック制御を行うクロックコントローラ3に対してキーストリームを出力している。クロックコントローラ3は、入力されたキーストリームに従いクロック（シフト量）を決定してLFSR-B(4)を制御する構成になっている。

40

【0025】

なお、非線形関数発生器6の出力であるキーストリームは、外部から供給される平文とXOR演算が実行され、暗号化されたテキストを出力する。ここでは、非線形関数発生器6とXOR演算器とを総称して暗号化処理部としている。暗号化処理部は、内部状態メモリ5に保持された内部状態を使用してキーストリームを生成し、当該キーストリームと外部から入力される平文とを演算して暗号化を行い、内部状態メモリ5に保持すべき内部状

50

態を動的に更新する。

【0026】

また、内部状態復元部7は、暗号化あるいは復号化が終了し、あるいは初期値(IV)の入力があった場合、内部状態メモリ5に逐一保持された内部状態を消去し、内部状態メモリ5に保存されている初期攪拌終了後の内部状態に復元する。

【0027】

以下、図3に示すストリーム暗号装置の動作について詳細に説明する。まず、LFSR-A(2)、LFSR-B(4)への内部状態の設定にあたり、内部状態生成部1へ秘密鍵(IK: Initial Key)と初期値(IV: Initial Value)が入力される。このとき、内部状態生成部1(第1の内部状態生成部)は、所定のキースケジュールアルゴリズムに従い内部状態を決定し、LFSR-A(2)、LFSR-B(4)のそれぞれに内部状態(第1の擬似乱数列、第2の擬似乱数列)を入力して初期化処理を実行する。このとき、決定された内部状態を内部状態メモリ5に保存する。

10

【0028】

続いて、内部状態生成部1(第2の内部状態生成部)は、上記した初期化処理における周期よりも短い周期で到来する初期値を受信し、当該初期値と内部状態メモリ5に保存された初期攪拌終了後の内部状態とを演算し、その結果を暗号化処理用として内部状態メモリ5に保持して簡易初期化処理を実行する

【0029】

上記した簡易初期化処理終了の後、本発明の実施形態にかかわるストリーム暗号装置は、以下の手順に従って暗号化処理を実行する。

20

すなわち、LFSR-B(4)により出力されるキーストリームは、後述するクロックコントローラ3によるクロック制御を経て非線形関数発生器6の入力として供給される。非線形関数発生器6は、入力されたキーストリームと、内部状態メモリ5に保存された内部状態とにより、ある非線形関数演算を実行して新たなキーストリームを生成する。そして、非線形関数発生器6により生成されるキーストリームは、別途入力される平文とによりXOR演算が施され、このことにより暗号化テキストが生成される。

【0030】

なお、内部状態は上記した暗号化処理の過程で適宜更新される。すなわち、非線形関数発生器6の出力は内部状態メモリ5にも供給されており、内容が更新された内部状態メモリ5の出力は非線形関数発生器6にフィードバックされ入力されている。また、LFSR-A(2)は、クロック制御を行うクロックコントローラ3に対して内部状態(擬似乱数列)を出力している。

30

【0031】

クロックコントローラ3は、入力されたキーストリーム(擬似乱数列)に従いクロックを決定してLFSR-B(4)を制御する。具体的に、ここでは、LFSR-A(2)、LFSR-B(4)を1周期動作させている。その際、クロックコントローラ3は、次数2のガロア有限フィールド($GF(2^n)$)を定義する多項式の根に従い、LFSR-B(4)のフィードバックポリノミアル(図3中結線部分)のビットシフトにクロック制御($\times n$ を掛ける)を行う。ここで、 n はクロックコントローラ3が決定したクロック数(シフト量)である。このことにより、1ワード内でのクロック制御が行なわれる。

40

【0032】

最後に、暗号化処理が終了し、あるいは新規に初期値(IV)入力があった場合、内部状態復元部7は、内部状態メモリ5に保持された内部状態を消去し、内部状態メモリ5に保存されている初期攪拌終了後の内部状態に基づき、上記した簡易初期化処理以降の処理の繰り返し実行を指示する。

【0033】

以上説明のように本発明は、通常の初期化処理が終了した内部状態と、暗号化処理時の内部状態を独立して管理し、暗号化処理時、上記した簡易初期化処理を実行して内部状態を更新した後に暗号化処理を行い、暗号化処理終了後にその内部状態を消去して通常の初

50

期化終了時の内部状態を復元することにより、頻繁に初期値が更新される環境にあっても、高速、かつ安全なストリーム暗号を実現するものである。

【0034】

本発明は、一定周期で初期値を送信し、途中から受信したユーザもストリーム暗号を用いて復元を行う放送データの暗号化の初期化処理に用いて特に顕著な効果が得られる。また、様々なストリーム暗号の評価に広く適用でき、ストリーム暗号を使用するようなブロードバンド事業や、携帯電話をはじめとするモバイル通信におけるシステム構築に 응용が可能である。

【図面の簡単な説明】

【0035】

【図1】本発明の実施形態にかかわるストリーム暗号方法の各実行手順を説明するために引用したフローチャートである。

【図2】本発明により付加される簡易初期化処理の詳細手順を説明するために引用したフローチャートである。

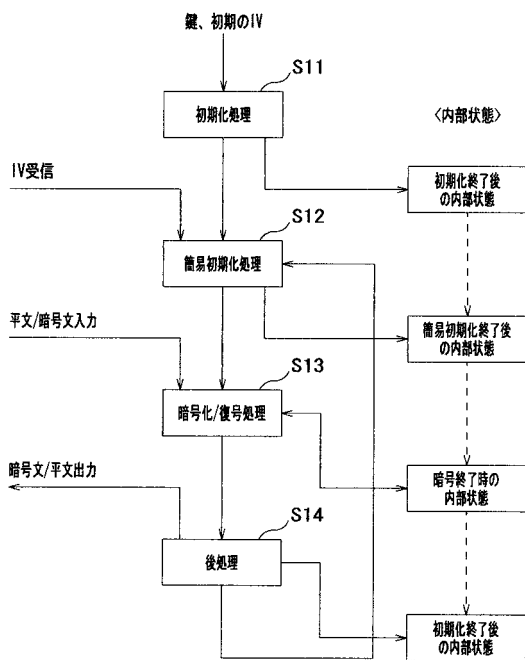
【図3】本発明の実施形態にかかわるストリーム暗号装置の内部構成を示すブロック図である。

【符号の説明】

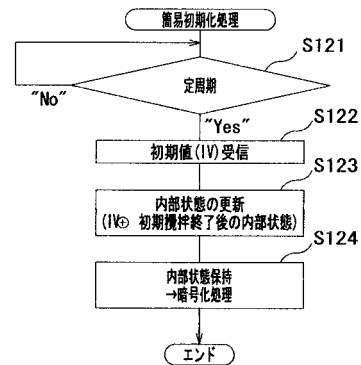
【0036】

1...内部状態生成部(第1、第2の内部状態生成部)、2、4...線形フィードバックレジスタ(LFSR-A, LFSR-B)、3...クロックコントローラ、5...内部状態メモリ、6...非線型関数発生器(暗号化処理部)、7...内部状態復元部

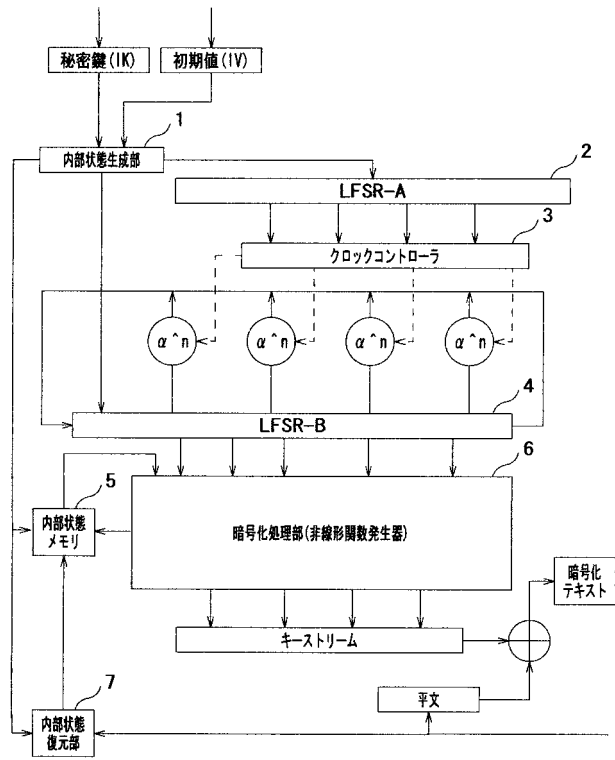
【図1】



【図2】



【 図 3 】



フロントページの続き

Fターム(参考) 5J104 AA01 FA01 FA05 JA03 JA04 NA02 NA23 NA37