

(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2006-186871

(P2006-186871A)

(43) 公開日 平成18年7月13日(2006.7.13)

(51) Int. Cl.	F I	テーマコード (参考)
H04L 9/08 (2006.01)	H04L 9/00 601B H04L 9/00 601E	5J104

審査請求 未請求 請求項の数 14 O L (全 24 頁)

(21) 出願番号 (22) 出願日	特願2004-380584 (P2004-380584) 平成16年12月28日 (2004.12.28)	(71) 出願人 504150450 国立大学法人神戸大学 兵庫県神戸市灘区六甲台町1-1
特許法第30条第1項適用申請有り 平成16年12月14日 情報理論とその応用学会発行の「第27回 情報理論とその応用シンポジウム予稿集」に発表		(74) 代理人 100084375 弁理士 板谷 康夫
		(72) 発明者 栗林 稔 神戸市灘区六甲台町1-1 神戸大学工学部内
		(72) 発明者 田中 初一 神戸市灘区六甲台町1-1 神戸大学工学部内
		Fターム(参考) 5J104 AA01 AA12 AA16 AA34 BA03 EA01 EA04 EA15 EA16 EA17 EA18 FA08 JA03 JA20 MA05 NA02 NA04 NA19 NA37 PA05 PA07

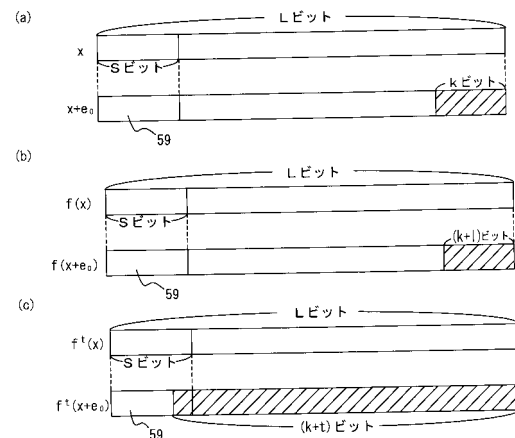
(54) 【発明の名称】ブロードキャスト型コンテンツ配信システム、及び同システムに適用されるユーザ鍵管理方法

(57) 【要約】

【課題】ブロードキャスト型コンテンツ配信システムにおいて、ユーザ管理に必要なコストの低減を図り、復号鍵の不正配布問題に有効に対処する。

【解決手段】ユーザ鍵の初期値 ($x + e_0$) が、その時点の最新のカオス系列 x に乱数を加算したものであることから、所定の時間経過する度に (ロジスティック写像を繰り返す度に)、最新のカオス系列の値と最新のユーザ鍵の値との誤差が、拡大していく。このため、所定の期間が経過するまでは、最新のカオス系列の上位 S ビットに基づいて生成された暗号鍵と、最新のユーザ鍵の上位 S ビットに基づいて生成された復号鍵とが一致するので、暗号化されたコンテンツを復号することができるが、所定の期間が経過すると (写像の繰返回数 t が増えると)、暗号鍵と復号鍵とが一致なくなり、暗号化されたコンテンツを復号できないようになる。このことは、実質的に、ユーザ鍵に有効期限を設けることと同じである。

【選択図】図5



【特許請求の範囲】

【請求項 1】

デジタルテレビジョン放送等のコンテンツの提供者側に設置された提供者側コンピュータと、この提供者側コンピュータとネットワークを介して接続されて、前記コンテンツの視聴者であるユーザ側に設置されたユーザ側情報端末とから構成され、前記提供者側コンピュータに登録されたユーザのみが、前記提供者側コンピュータから配信されたコンテンツを復元して視聴することが可能なブロードキャスト型のコンテンツ配信システムにおいて、

前記提供者側コンピュータは、コンテンツの暗号鍵の生成元となるカオス系列の初期値を生成する初期値生成手段と、

前記初期値生成手段により生成された初期値に対して、カオス写像のうちの、誤差の伝播のスピードがほぼ一定の写像を 回（ただし、 は 1 以上の整数）行って、最新のカオス系列を求めた後に、所定の時間が経過する度に、その時点の最新のカオス系列に対して、前記カオス写像と同じカオス写像を 回繰り返して、最新のカオス系列を求めるカオス系列更新手段と、

前記カオス系列更新手段により求められた最新のカオス系列を 2 進数で表し、この 2 進数を構成する上位の n ビット（ただし、 n は 1 以上の整数）のうち、所定数以上のビットを抽出して、コンテンツを暗号化するための暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵生成手段により生成された暗号鍵を用いて、コンテンツを暗号化する暗号化手段と、

前記暗号化手段により暗号化されたコンテンツを前記ユーザ側情報端末に送信するコンテンツ送信手段と、

前記ユーザ側情報端末からのユーザ登録要求のデータの受信時に、前記カオス系列更新手段により求められた、その時点の最新のカオス系列に乱数を加算して、ユーザ鍵を生成するユーザ鍵生成手段と、

前記ユーザ鍵生成手段により生成されたユーザ鍵を前記ユーザ側情報端末に送信するユーザ鍵送信手段とを備え、

前記ユーザ側情報端末は、前記提供者側コンピュータにユーザ登録要求のデータを送信する登録要求送信手段と、

前記提供者側コンピュータから送信されたユーザ鍵を受信するユーザ鍵受信手段と、

前記ユーザ鍵受信手段により受信したユーザ鍵を初期状態における最新のユーザ鍵として、所定の時間経過する度に、その時点の最新のユーザ鍵に対して、前記カオス写像と同じカオス写像を 回繰り返して、最新のユーザ鍵を求めるユーザ鍵更新手段と、

前記ユーザ鍵更新手段により求められた最新のユーザ鍵を 2 進数で表し、この 2 進数に対して、前記暗号鍵生成手段におけるビット抽出処理と同じ内容のビット抽出処理を行って、暗号化されたコンテンツを復号するための復号鍵を生成する復号鍵生成手段と、

前記提供者側コンピュータから送信された暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記復号鍵生成手段により生成された復号鍵を用いて、前記コンテンツ受信手段により受信した暗号化されたコンテンツを復号する復号手段とを備え、

前記暗号化手段は、前記暗号化処理を共通鍵暗号方式で行い、

前記復号鍵生成手段により生成された復号鍵が、前記暗号鍵生成手段により生成された暗号鍵と一致する間は、前記復号手段による復号を可能にし、前記復号鍵生成手段により生成された復号鍵が、前記暗号鍵生成手段により生成された暗号鍵と一致しなくなった場合には、前記復号手段による復号を不可能にすることにより、ユーザ鍵に有効期限を設けたことを特徴とするブロードキャスト型コンテンツ配信システム。

【請求項 2】

前記カオス系列更新手段により用いられたカオス写像は、ロジスティック写像であることを特徴とする請求項 1 に記載のブロードキャスト型コンテンツ配信システム。

【請求項 3】

前記暗号鍵生成手段は、前記カオス系列更新手段により求められた最新のカオス系列を2進数で表し、この2進数を構成する上位のnビットを抽出して、コンテンツを暗号化するための暗号鍵を生成することを特徴とする請求項1又は請求項2に記載のブロードキャスト型コンテンツ配信システム。

【請求項4】

前記初期値生成手段により生成された初期値は、ビット長が256以上の2進数で表されることを特徴とする請求項2に記載のブロードキャスト型コンテンツ配信システム。

【請求項5】

前記カオス系列更新手段によるカオス写像の繰り返しの回数である は、16以上であることを特徴とする請求項4に記載のブロードキャスト型コンテンツ配信システム。

10

【請求項6】

前記提供者側コンピュータのユーザ鍵送信手段は、ユーザ鍵と一緒に、ユーザ鍵の有効期限を表すデータを、前記ユーザ側情報端末に送信し、

前記ユーザ側情報端末のユーザ鍵受信手段は、前記ユーザ鍵の有効期限を表すデータを受信し、

前記ユーザ側情報端末は、

前記ユーザ鍵の有効期限を表すデータに基づいて、ユーザ鍵の有効期限が切れたか否かを判定する期限切れ判定手段と、

前記期限切れ判定手段によりユーザ鍵の有効期限が切れたと判定されたときに、有効期限が切れる前に前記ユーザ鍵更新手段により算出されたユーザ鍵のうちの最後に算出されたユーザ鍵に対して、前記ユーザ鍵更新手段により用いられたカオス写像と同じカオス写像を 回(ただし、 は1以上の整数)繰り返して、新たなカオス系列を求めた上で、このカオス系列の上位nビット(ただし、 nは1以上の整数)を抽出することにより、再登録ユーザであることの証明データを生成する再登録証明データ生成手段と、

20

前記再登録証明データ生成手段により生成された証明データを前記提供者側コンピュータに送信する証明データ送信手段とをさらに備え、

前記提供者側コンピュータは、前記ユーザ側情報端末から送信された証明データに基づいて、この証明データを送信したユーザが過去にユーザ登録をしたことのあるユーザであるか否かを判別する判別手段をさらに備えたことを特徴とする請求項1乃至請求項5に記載のブロードキャスト型コンテンツ配信システム。

30

【請求項7】

前記ユーザ側情報端末は、デジタルテレビジョン放送信号受信機であり、前記コンテンツ送信手段は、前記暗号化手段により暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式で前記デジタルテレビジョン放送信号受信機に送信することを特徴とする請求項1乃至請求項6に記載のブロードキャスト型コンテンツ配信システム。

【請求項8】

デジタルテレビジョン放送等のコンテンツの提供者側に設置された提供者側コンピュータと、この提供者側コンピュータとネットワークを介して接続されて、前記コンテンツの視聴者であるユーザ側に設置されたユーザ側情報端末とから構成されたブロードキャスト型のコンテンツ配信システムに適用される、ユーザ鍵の管理方法において、

40

前記提供者側コンピュータが、コンテンツの暗号鍵の生成元となるカオス系列の初期値を生成するステップ、

前記提供者側コンピュータが、前記生成された初期値を用いて、所定の時間が経過する度に、カオス写像のうちの、誤差の伝播のスピードがほぼ一定の写像を 回(ただし、 は1以上の整数)行って、最新のカオス系列を求めるステップ、

前記提供者側コンピュータが、前記最新のカオス系列を2進数で表し、この2進数を構成する上位のnビット(ただし、 nは1以上の整数)のうち、所定数以上のビットを抽出して、コンテンツを暗号化するための暗号鍵を生成するステップ、

前記提供者側コンピュータが、前記暗号鍵を用いて、コンテンツを暗号化するステップ

50

、
前記提供者側コンピュータが、暗号化されたコンテンツを前記ユーザ側情報端末に送信するステップ、

前記ユーザ側情報端末が、前記提供者側コンピュータにユーザ登録要求のデータを送信するステップ、

前記提供者側コンピュータが、前記ユーザ側情報端末からのユーザ登録要求のデータの受信時に、その時点の最新のカオス系列に乱数を加算して、ユーザ鍵を生成するステップ

、
前記提供者側コンピュータが、前記ユーザ鍵を前記ユーザ側情報端末に送信するステップ、

前記ユーザ側情報端末が、前記提供者側コンピュータから送信されたユーザ鍵を受信するステップ、

前記ユーザ側情報端末が、前記受信したユーザ鍵を初期値として用いて、所定の時間が経過する度に、前記提供者側コンピュータにおける最新のカオス系列の算出に用いられたカオス写像と同じカオス写像を 1 回行って、最新のユーザ鍵を求めるステップ、

前記ユーザ側情報端末が、前記最新のユーザ鍵を 2 進数で表し、この 2 進数に対して、前記提供者側コンピュータにおける暗号鍵を生成するステップで行われたビット抽出処理と同じ内容のビット抽出処理を行って、暗号化されたコンテンツを復号するための復号鍵を生成するステップ、

前記ユーザ側情報端末が、前記提供者側コンピュータから送信された暗号化されたコンテンツを受信するステップ、及び

前記ユーザ側情報端末が、前記復号鍵を用いて、前記提供者側コンピュータから受信した暗号化されたコンテンツを復号するステップからなり、

前記暗号化するステップにおける暗号化処理は、共通鍵暗号方式で行われ、

前記復号鍵を生成するステップにおいて生成された復号鍵が、前記暗号鍵を生成するステップにおいて生成された暗号鍵と一致する間は、前記提供者側コンピュータから受信した暗号化されたコンテンツの復号を可能にし、前記復号鍵を生成するステップにおいて生成された復号鍵が、前記暗号鍵を生成するステップにおいて生成された暗号鍵と一致しなくなった場合には、前記提供者側コンピュータから受信した暗号化されたコンテンツの復号を不可能にすることにより、ユーザ鍵に有効期限を設けたことを特徴とする、ブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【請求項 9】

前記最新のカオス系列を求めるステップにおいて用いられたカオス写像は、ロジスティック写像であることを特徴とする請求項 8 に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【請求項 10】

前記暗号鍵を生成するステップにおいて、前記最新のカオス系列を求めるステップで求められた最新のカオス系列を 2 進数で表し、この 2 進数を構成する上位の n ビットを抽出して、コンテンツを暗号化するための暗号鍵を生成することを特徴とする請求項 8 又は請求項 9 に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【請求項 11】

前記初期値を生成するステップにおいて生成された初期値は、ビット長が 256 以上の 2 進数で表されることを特徴とする請求項 9 に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【請求項 12】

前記最新のカオス系列を求めるステップにおける、カオス写像の繰り返しの回数 は、16 以上であることを特徴とする請求項 11 に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【請求項 13】

10

20

30

40

50

前記提供者側コンピュータは、前記ユーザ鍵を送信するステップにおいて、ユーザ鍵と一緒に、ユーザ鍵の有効期限を表すデータを、前記ユーザ側情報端末に送信し、

前記ユーザ側情報端末は、前記ユーザ鍵を受信するステップにおいて、前記ユーザ鍵の有効期限を表すデータを受信し、

前記ユーザ側情報端末が、前記ユーザ鍵の有効期限を表すデータに基づいて、ユーザ鍵の有効期限が切れたか否かを判定するステップと、

前記ユーザ側情報端末が、前記判定するステップにおいてユーザ鍵の有効期限が切れたと判定されたときに、有効期限が切れる前に算出されたユーザ鍵のうちの最後に算出されたユーザ鍵に対して、前記最新のユーザ鍵を求めるステップにおいて用いられたカオス写像と同じカオス写像を 回（ただし、 n は 1 以上の整数）繰り返して、新たなカオス系列を求めた上で、このカオス系列の上位 n ビット（ただし、 n は 1 以上の整数）を抽出することにより、再登録ユーザであることの証明データを生成するステップと、

前記ユーザ側情報端末が、前記証明データを送信するステップと、

前記提供者側コンピュータが、前記ユーザ側情報端末から送信された証明データに基づいて、この証明データを送信したユーザが過去にユーザ登録をしたことのあるユーザであるか否かを判別するステップとをさらに有することを特徴とする請求項 8 乃至請求項 12 に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【請求項 14】

前記ユーザ側情報端末は、デジタルテレビジョン放送信号受信機であり、前記コンテンツを送信するステップにおいて、暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式で前記デジタルテレビジョン放送信号受信機に送信することを特徴とする請求項 8 乃至請求項 13 に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ブロードキャスト型コンテンツ配信システム、及び同システムに適用されるユーザ鍵管理方法に係り、特に、提供者側から配信されたコンテンツを視聴することが可能なユーザを限定する技術に関する。

【背景技術】

【0002】

従来より、デジタルテレビジョン放送等のコンテンツの配信システムでは、コンテンツの提供者側のコンピュータ（以下、提供者側コンピュータという）に登録されたユーザのみが、この提供者側コンピュータから配信された、暗号化されたコンテンツを復元して視聴することができるようにしたものが一般的である。このような仕組みを実現するために、種々のブロードキャスト暗号システムが提案されている。一般に、ブロードキャスト暗号システムにおいては、リアルタイム再生可能なプログラムを実現する必要上、コンテンツの暗号化と復号化を迅速に行わなければならない。従って、ブロードキャスト暗号システムでは、公開鍵暗号方式に比べて暗号化・復号化の処理速度が速い共通鍵（秘密鍵）暗号方式が採用されている。

【0003】

ところが、一般に、共通鍵暗号方式では、共通鍵の管理に手間がかかるという問題がある。すなわち、共通鍵暗号方式では、情報の送信者、受信者の両方が同一の鍵を所有しなければならないし、第三者には鍵を秘密にしておかななければならないので、1組の送信者、受信者毎に別々の共通鍵を持つことになる。従って、ユーザは、多くの相手と暗号化通信を行う場合には、所有する共通鍵の数も多くなるので、共通鍵の管理に手間がかかる。

【0004】

上記のように、ブロードキャスト暗号システムでは、共通鍵暗号方式を採用する必要があることから、上記の共通鍵暗号方式に関する問題は、ブロードキャスト暗号システムの問題でもある。すなわち、ブロードキャスト暗号システムでは、コンテンツの視聴者であ

10

20

30

40

50

るユーザ毎に共通鍵が異なるので、提供者側コンピュータは、各ユーザ毎に異なる共通鍵（暗号鍵）で異なるコンテンツの暗号文を作成する必要があった。また、ユーザ登録の期限が切れた場合には、該当ユーザの情報端末（以下、ユーザ側情報端末という）との通信等の処理を行って、該当ユーザの共通鍵を使用できなくなるようにする必要があるので、各ユーザの共通鍵の管理に必要な処理が多くなる。このため、提供者側において、ユーザ管理に必要な計算処理とコンピュータ資源の量が多くなるので、ユーザ管理に必要なコストが高くなるという問題があった。

【0005】

また、上記のブロードキャスト暗号システムには、共通鍵の不正配布の問題があった。すなわち、上記システムでは、登録ユーザが、非登録ユーザに秘密の共通鍵を配布してしまうおそれがあった。この不正配布を防ぐために、下記の特許文献1は、不正者追跡の仕組み（Traitor Tracing Scheme）を開示している。この仕組みは、コンテンツの提供者が、不正に配布された鍵に基づいて不正配布を行った登録ユーザを識別できるようにしたものである。上記の不正者追跡の仕組みにおいては、提供者側コンピュータからユーザ側情報端末に送信されるデータは、2つの暗号文から構成されている。1つの暗号文は、コンテンツを暗号化するための鍵（SEK（session-encrypting key））の暗号文であり、もう1つの暗号文は、このSEKを用いて暗号化されたコンテンツの暗号文である。上記のSEKの暗号文を復号することができるのは、各自の復号鍵（KEK（key-encrypting key））を持つ登録ユーザのみである。各ユーザのKEKは、識別可能であるため、コンテンツの提供者は、KEKの所有者を特定することができる。

10

20

【0006】

ところが、上記のような不正者追跡の仕組みにおいて、ユーザ固有の復号鍵に基づいて、復号鍵を不正配布した不正者を追跡するためには、コンテンツの提供者は、ネットワーク上において、復号鍵自体が、登録ユーザと非登録ユーザとの間の取り引きを検出しなければならない。しかし、このような不正な取り引きは、提供者による検出を逃れるために、狡猾な方法で行われることが多く、しかも、その回数が多くはない。従って、上記のような不正者追跡の仕組みでは、不正者を検挙することができる確率が低いため、復号鍵の不正配布の問題に有効に対処することができない。

【非特許文献1】チョー（B.Chor）、外3名、「不正者追跡（Tracing traitors）」、トランスインフォームセオリー（Transactions on Information Theory）（アメリカ合衆国）、電気電子技術者協会（Institute of Electrical and Electronics Engineers）、2000年、第46巻、第3号、p893-910

30

【発明の開示】

【発明が解決しようとする課題】

【0007】

本発明は、上記の問題を解決するためになされたものであり、コンテンツの提供者が、従来のブロードキャスト暗号システムを採用したブロードキャスト型コンテンツ配信システムと比べて、ユーザ管理に必要なコストの低減を図ることができ、しかも、復号鍵の不正配布問題に有効に対処することが可能なブロードキャスト型コンテンツ配信システムを提供することを目的とする。

40

【課題を解決するための手段】

【0008】

上記目的を達成するために請求項1の発明は、デジタルテレビジョン放送等のコンテンツの提供者側に設置された提供者側コンピュータと、この提供者側コンピュータとネットワークを介して接続されて、前記コンテンツの視聴者であるユーザ側に設置されたユーザ側情報端末とから構成され、前記提供者側コンピュータに登録されたユーザのみが、前記提供者側コンピュータから配信されたコンテンツを復元して視聴することが可能なブロードキャスト型のコンテンツ配信システムにおいて、前記提供者側コンピュータは、コンテンツの暗号鍵の生成元となるカオス系列の初期値を生成する初期値生成手段と、前記初期値生成手段により生成された初期値に対して、カオス写像のうちの、誤差の伝播のスビ

50

ードがほぼ一定の写像を 回（ただし、 は 1 以上の整数）行って、最新のカオス系列を求めた後に、所定の時間が経過する度に、その時点の最新のカオス系列に対して、前記カオス写像と同じカオス写像を 回繰り返して、最新のカオス系列を求めるカオス系列更新手段と、前記カオス系列更新手段により求められた最新のカオス系列を 2 進数で表し、この 2 進数を構成する上位の n ビット（ただし、 n は 1 以上の整数）のうち、所定数以上のビットを抽出して、コンテンツを暗号化するための暗号鍵を生成する暗号鍵生成手段と、前記暗号鍵生成手段により生成された暗号鍵を用いて、コンテンツを暗号化する暗号化手段と、前記暗号化手段により暗号化されたコンテンツを前記ユーザ側情報端末に送信するコンテンツ送信手段と、前記ユーザ側情報端末からのユーザ登録要求のデータの受信時に、前記カオス系列更新手段により求められた、その時点の最新のカオス系列に乱数を加算して、ユーザ鍵を生成するユーザ鍵生成手段と、前記ユーザ鍵生成手段により生成されたユーザ鍵を前記ユーザ側情報端末に送信するユーザ鍵送信手段とを備え、前記ユーザ側情報端末は、前記提供者側コンピュータにユーザ登録要求のデータを送信する登録要求送信手段と、前記提供者側コンピュータから送信されたユーザ鍵を受信するユーザ鍵受信手段と、前記ユーザ鍵受信手段により受信したユーザ鍵を初期状態における最新のユーザ鍵として、所定の時間経過する度に、その時点の最新のユーザ鍵に対して、前記カオス写像と同じカオス写像を 回繰り返して、最新のユーザ鍵を求めるユーザ鍵更新手段と、前記ユーザ鍵更新手段により求められた最新のユーザ鍵を 2 進数で表し、この 2 進数に対して、前記暗号鍵生成手段におけるビット抽出処理と同じ内容のビット抽出処理を行って、暗号化されたコンテンツを復号するための復号鍵を生成する復号鍵生成手段と、前記提供者側コンピュータから送信された暗号化されたコンテンツを受信するコンテンツ受信手段と、前記復号鍵生成手段により生成された復号鍵を用いて、前記コンテンツ受信手段により受信した暗号化されたコンテンツを復号する復号手段とを備え、前記暗号化手段は、前記暗号化処理を共通鍵暗号方式で行い、前記復号鍵生成手段により生成された復号鍵が、前記暗号鍵生成手段により生成された暗号鍵と一致する間は、前記復号手段による復号を可能にし、前記復号鍵生成手段により生成された復号鍵が、前記暗号鍵生成手段により生成された暗号鍵と一致しなくなった場合には、前記復号手段による復号を不可能にすることにより、ユーザ鍵に有効期限を設けたものである。

【0009】

請求項 2 の発明は、請求項 1 に記載のブロードキャスト型コンテンツ配信システムにおいて、前記カオス系列更新手段により用いられたカオス写像は、ロジスティック写像であるものである。

【0010】

請求項 3 の発明は、請求項 1 又は請求項 2 に記載のブロードキャスト型コンテンツ配信システムにおいて、前記暗号鍵生成手段は、前記カオス系列更新手段により求められた最新のカオス系列を 2 進数で表し、この 2 進数を構成する上位の n ビットを抽出して、ブロードキャスト型コンテンツを暗号化するための暗号鍵を生成するものである。

【0011】

請求項 4 の発明は、請求項 2 に記載のブロードキャスト型コンテンツ配信システムにおいて、前記初期値生成手段により生成された初期値は、ビット長が 256 以上の 2 進数で表されるものである。

【0012】

請求項 5 の発明は、請求項 4 に記載のブロードキャスト型コンテンツ配信システムにおいて、前記カオス系列更新手段によるカオス写像の繰り返しの回数である は、16 以上であるものである。

【0013】

請求項 6 の発明は、請求項 1 乃至請求項 5 に記載のブロードキャスト型コンテンツ配信システムにおいて、前記提供者側コンピュータのユーザ鍵送信手段は、ユーザ鍵と一緒に、ユーザ鍵の有効期限を表すデータを、前記ユーザ側情報端末に送信し、前記ユーザ側情報端末のユーザ鍵受信手段は、前記ユーザ鍵の有効期限を表すデータを受信し、前記ユー

ザ側情報端末は、前記ユーザ鍵の有効期限を表すデータに基づいて、ユーザ鍵の有効期限が切れたか否かを判定する期限切れ判定手段と、前記期限切れ判定手段によりユーザ鍵の有効期限が切れたと判定されたときに、有効期限が切れる前に前記ユーザ鍵更新手段により算出されたユーザ鍵のうちの最後に算出されたユーザ鍵に対して、前記ユーザ鍵更新手段により用いられたカオス写像と同じカオス写像を 回（ただし、 は 1 以上の整数）繰り返し返して、新たなカオス系列を求めた上で、このカオス系列の上位 n ビット（ただし、 n は 1 以上の整数）を抽出することにより、再登録ユーザであることの証明データを生成する再登録証明データ生成手段と、前記再登録証明データ生成手段により生成された証明データを送信する証明データ送信手段とをさらに備え、前記提供者側コンピュータは、前記ユーザ側情報端末から送信された証明データに基づいて、この証明データを送信したユーザが過去にユーザ登録をしたことのあるユーザであるか否かを判別する判別手段をさらに備えたものである。

10

【0014】

請求項 7 の発明は、請求項 1 乃至請求項 6 に記載のブロードキャスト型コンテンツ配信システムにおいて、前記ユーザ側情報端末は、デジタルテレビジョン放送信号受信機であり、前記コンテンツ送信手段は、前記暗号化手段により暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式で前記デジタルテレビジョン放送信号受信機に送信するものである。

【0015】

請求項 8 の発明は、デジタルテレビジョン放送等のコンテンツの提供者側に設置された提供者側コンピュータと、この提供者側コンピュータとネットワークを介して接続されて、前記コンテンツの視聴者であるユーザ側に設置されたユーザ側情報端末とから構成されたブロードキャスト型のコンテンツ配信システムに適用される、ユーザ鍵の管理方法において、前記提供者側コンピュータが、コンテンツの暗号鍵の生成元となるカオス系列の初期値を生成するステップ、前記提供者側コンピュータが、前記生成された初期値を用いて、所定の時間が経過する度に、カオス写像のうちの、誤差の伝播のスピードがほぼ一定の写像を 回（ただし、 は 1 以上の整数）行って、最新のカオス系列を求めるステップ、前記提供者側コンピュータが、前記最新のカオス系列を 2 進数で表し、この 2 進数を構成する上位の n ビット（ただし、 n は 1 以上の整数）のうち、所定数以上のビットを抽出して、コンテンツを暗号化するための暗号鍵を生成するステップ、前記提供者側コンピュータが、前記暗号鍵を用いて、コンテンツを暗号化するステップ、前記提供者側コンピュータが、暗号化されたコンテンツを前記ユーザ側情報端末に送信するステップ、前記ユーザ側情報端末が、前記提供者側コンピュータにユーザ登録要求のデータを送信するステップ、前記提供者側コンピュータが、前記ユーザ側情報端末からのユーザ登録要求のデータの受信時に、その時点の最新のカオス系列に乱数を加算して、ユーザ鍵を生成するステップ、前記提供者側コンピュータが、前記ユーザ鍵を前記ユーザ側情報端末に送信するステップ、前記ユーザ側情報端末が、前記提供者側コンピュータから送信されたユーザ鍵を受信するステップ、前記ユーザ側情報端末が、前記受信したユーザ鍵を初期値として用いて、所定の時間が経過する度に、前記提供者側コンピュータにおける最新のカオス系列の算出に用いられたカオス写像と同じカオス写像を 回行って、最新のユーザ鍵を求めるステップ、前記ユーザ側情報端末が、前記最新のユーザ鍵を 2 進数で表し、この 2 進数に対して、前記提供者側コンピュータにおける暗号鍵を生成するステップで行われたビット抽出処理と同じ内容のビット抽出処理を行って、暗号化されたコンテンツを復号するための復号鍵を生成するステップ、前記ユーザ側情報端末が、前記提供者側コンピュータから送信された暗号化されたコンテンツを受信するステップ、及び前記ユーザ側情報端末が、前記復号鍵を用いて、前記提供者側コンピュータから受信した暗号化されたコンテンツを復号するステップからなり、前記暗号化するステップにおける暗号化処理は、共通鍵暗号方式で行われ、前記復号鍵を生成するステップにおいて生成された復号鍵が、前記暗号鍵を生成するステップにおいて生成された暗号鍵と一致する間は、前記提供者側コンピュータから受信した暗号化されたコンテンツの復号を可能にし、前記復号鍵を生成するステップに

20

30

40

50

において生成された復号鍵が、前記暗号鍵を生成するステップにおいて生成された暗号鍵と一致しなくなった場合には、前記提供者側コンピュータから受信した暗号化されたコンテンツの復号を不可能にすることにより、ユーザ鍵に有効期限を設けたものである。

【0016】

請求項9の発明は、請求項8に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法において、前記最新のカオス系列を求めるステップにおいて用いられたカオス写像は、ロジスティック写像であるものである。

【0017】

請求項10の発明は、請求項8又は請求項9に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法において、前記暗号鍵を生成するステップにおいて、前記最新のカオス系列を求めるステップで求められた最新のカオス系列を2進数で表し、この2進数を構成する上位のnビットを抽出して、ブロードキャスト型コンテンツを暗号化するための暗号鍵を生成するものである。

10

【0018】

請求項11の発明は、請求項9に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法において、前記初期値を生成するステップにおいて生成された初期値は、ビット長が256以上の2進数で表されるものである。

【0019】

請求項12の発明は、請求項11に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法において、前記最新のカオス系列を求めるステップにおける、カオス写像の繰り返しの回数は、16以上であるものである。

20

【0020】

請求項13の発明は、請求項8乃至請求項12に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法において、前記提供者側コンピュータは、前記ユーザ鍵を送信するステップにおいて、ユーザ鍵と一緒に、ユーザ鍵の有効期限を表すデータを、前記ユーザ側情報端末に送信し、前記ユーザ側情報端末は、前記ユーザ鍵を受信するステップにおいて、前記ユーザ鍵の有効期限を表すデータを受信し、前記ユーザ側情報端末が、前記ユーザ鍵の有効期限を表すデータに基づいて、ユーザ鍵の有効期限が切れたか否かを判定するステップと、前記ユーザ側情報端末が、前記判定するステップにおいてユーザ鍵の有効期限が切れたと判定されたときに、有効期限が切れる前に算出されたユーザ鍵のうちの最後に算出されたユーザ鍵に対して、前記最新のカオス系列を求めるステップにおいて用いられたカオス写像と同じカオス写像を回(ただし、は1以上の整数)繰り返して、新たなカオス系列を求めた上で、このカオス系列の上位nビット(ただし、nは1以上の整数)を抽出することにより、再登録ユーザであることの証明データを生成するステップと、前記ユーザ側情報端末が、前記証明データを送信するステップと、前記提供者側コンピュータが、前記ユーザ側情報端末から送信された証明データに基づいて、この証明データを送信したユーザが過去にユーザ登録をしたことのあるユーザであるかを判別するステップとをさらに有するものである。

30

【0021】

請求項14の発明は、請求項8乃至請求項13に記載のブロードキャスト型コンテンツ配信システムに適用されるユーザ鍵管理方法において、前記ユーザ側情報端末は、デジタルテレビジョン放送信号受信機であり、前記コンテンツを送信するステップにおいて、暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式で前記デジタルテレビジョン放送信号受信機に送信するものである。

40

【発明の効果】

【0022】

請求項1又は請求項8の発明によれば、提供者側コンピュータにおいて最新のカオス系列の算出に用いられるカオス写像と、ユーザ側情報端末において最新のユーザ鍵の算出に用いられるカオス写像とは、同じ写像であり、しかも、誤差の伝播のスピードがほぼ一定の写像である。従って、ユーザ鍵の初期値が、その時点の最新のカオス系列に乱数を加算

50

したものであることから、所定の時間経過する度に、最新のカオス系列の値と最新のユーザ鍵の値との誤差が、拡大していく。このため、所定の期間が経過するまでは、最新のカオス系列の上位の n ビットに基づいて生成された暗号鍵と、最新のユーザ鍵の上位の n ビットに基づいて生成された復号鍵とが一致するので、暗号化されたコンテンツを復号することができるが、所定の期間が経過すると、最新のカオス系列の上位の n ビットと最新のユーザ鍵の上位の n ビットとが一致しなくなるため、暗号鍵と復号鍵とが一致しなくなり、暗号化されたコンテンツを復号することができなくなってしまう。このことは、実質的に、ユーザ鍵に有効期限を設けることと同じである。

【0023】

上記のようにしたことにより、ユーザ登録の期限（ユーザ鍵の有効期限）が切れた場合でも、提供者側コンピュータが、該当ユーザのユーザ側情報端末との通信等の処理を行って、該当ユーザのユーザ鍵を使用できなくなるようにする必要がなくなる。また、提供者側コンピュータは、その時点の最新のカオス系列に基づき生成した同一の暗号鍵を用いて、全てのユーザ側情報端末に送信するコンテンツを暗号化することができるので、ユーザ毎に異なる暗号鍵でコンテンツを暗号化した場合と異なり、各ユーザ側情報端末毎に異なるコンテンツの暗号文を送信する必要がなくなる。すなわち、提供者側コンピュータがユーザ管理を行うために必要な処理を、ユーザ登録時におけるユーザ鍵の生成処理だけに行うことができる。従って、従来ブロードキャスト暗号システムを採用したブロードキャスト型コンテンツ配信システムと比べて、ユーザ管理に必要なコストの低減を図ることができる。

10

20

【0024】

また、上記のように、ユーザ鍵に有効期限を設けたことにより、ユーザ鍵の発行から所定の期間が経過すると、ユーザ鍵に基づいて生成される復号鍵が使用できなくなってしまうので、ユーザ鍵が不正に配布された場合でも、その影響を最小限に止めることができる。また、上記のようにユーザ鍵に有効期限を設けたことにより、不正配布者は、ユーザ鍵を非登録ユーザに頻りに配布しなければならなくなるので、提供者がユーザ鍵の不正配布を検出することができる可能性を高めることができる。すなわち、復号鍵の不正配布問題に有効に対処することができる。

【0025】

請求項2又は請求項9の発明によれば、カオス系列とユーザ鍵の更新に用いるカオス写像を、誤差の伝播のスピードがほぼ一定であるロジスティック写像としたことにより、上記の効果を的確に得ることができる。

30

【0026】

請求項3又は請求項10の発明によれば、最新のカオス系列を2進数で表し、この2進数を構成する上位の n ビットを抽出して、コンテンツを暗号化するための暗号鍵を生成するようにした。これにより、上記の効果を的確に得ることができる。

【0027】

請求項4又は請求項11の発明によれば、カオス系列の初期値を、ビット長が256以上の2進数で表されるものとしたことにより、カオス系列更新手段によるカオス系列の更新とユーザ鍵更新手段によるユーザ鍵の更新とを毎日行った場合でも、ユーザ鍵の有効期限をある程度長い期間に設定することが可能となる。

40

【0028】

請求項5又は請求項12の発明によれば、上記のカオス写像の繰り返しの回数であるを、16以上にしたことにより、総当たり攻撃に対して、ある程度の耐性を持つことができる。

【0029】

請求項6又は請求項13の発明によれば、ユーザ側情報端末が、ユーザ鍵の有効期限が切れたときに、有効期限が切れる前に算出されたユーザ鍵のうちの最後に算出されたユーザ鍵に対して、このユーザ鍵の算出に用いられたカオス写像と同じカオス写像を回繰り返して、新たなカオス系列を求めた上で、このカオス系列の上位 n ビットを抽出すること

50

により、再登録ユーザであることの証明データを生成し、生成された証明データを提供者側コンピュータに送信する。そして、提供者側コンピュータは、ユーザ側情報端末から送信された証明データに基づいて、この証明データを送信したユーザが過去にユーザ登録をしたことのあるユーザであるか否かを判別する。これにより、提供者側コンピュータが、証明データを送信したユーザが過去にユーザ登録をしたことのあるユーザであることを確認することができるので、過去に登録したことのあるユーザだけに対して登録料の割引を行うようにすることが可能となる。

【0030】

請求項7又は請求項14の発明によれば、暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式でデジタルテレビジョン放送信号受信機に送信するようにしたことにより、地上波デジタルテレビジョン放送やBSデジタル放送等の配信システムに本発明を適用することができる。

10

【発明を実施するための最良の形態】

【0031】

本発明を実施するための最良の形態について図面を参照して説明する。本発明は、ブロードキャスト型コンテンツ配信システム、及び同システムに適用されるユーザ鍵管理方法に係り、特に、提供者側から配信されたコンテンツを視聴することが可能なユーザを限定する技術に関するものである。以下に記載した実施形態は、本発明を網羅するものではなく、本発明は、下記の形態だけに限定されない。

【0032】

図1は、本実施形態によるブロードキャスト型コンテンツ配信システムにおける処理の概略を示す。ブロードキャスト型コンテンツ配信システム1（以下、コンテンツ配信システムと略す）は、デジタルテレビジョン放送等のコンテンツ6の提供者側に設置された提供者側サーバ2（提供者側コンピュータ）と、この提供者側サーバ2にネットワーク5を介して接続されて、コンテンツ6の視聴者であるユーザ側に設置されたユーザ側情報端末3a, 3bとから構成されている。ユーザ側情報端末3a, 3bは、パソコンであってもよいし、デジタルテレビジョン放送信号受信機であってもよい。ユーザ側情報端末3a, 3bをデジタルテレビジョン放送信号受信機とした場合には、提供者側サーバ2は、暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式でデジタルテレビジョン放送信号受信機に送信する。また、ネットワーク5は、インターネット等の有線のネットワークであってもよいし、無線のネットワークであってもよい。

20

30

【0033】

上記のコンテンツ配信システム1は、提供者側サーバ2に登録されたユーザのみが、提供者側サーバ2から配信されたコンテンツの暗号文7を復元して視聴することができるタイプのものである。このコンテンツ配信システム1では、提供者側サーバ2がユーザ管理を行うために必要な処理を、ユーザ登録時におけるユーザ鍵 U_0 の発行処理だけに行うことができる。従って、従来のコンテンツ配信システムと比べて、ユーザ管理に必要なコストの低減を図ることができる。提供者側サーバ2は、所定の時間（例えば、24時間）経過する度に、暗号鍵の元になるカオス系列 K_T を更新して、更新後のカオス系列 K_T のうちの上位 n ビットを、新たな暗号鍵とする。これに合わせて、ユーザ側情報端末3a, 3bも、上記のカオス系列 K_T の更新の間隔と同じ間隔で、所定の時間（例えば、24時間）経過する度に、復号鍵の元になるユーザ鍵 U_T を更新して、更新後のユーザ鍵 U_T のうちの上位 n ビットを、新たな復号鍵とする。ユーザ登録の有効期限内は、暗号鍵と復号鍵とが一致するので、コンテンツ6を復号することができるが、ユーザ登録の有効期限が切れると、暗号鍵と復号鍵とが一致しなくなり、コンテンツの暗号文7を復号することができなくなる。図に示されるユーザ側情報端末3bのように、ユーザ登録の有効期限が切れた端末は、提供者側サーバ2に再度ユーザ登録をした後でなければ、使用することができない。また、情報端末4のように、ユーザ登録をしていない者の情報端末は、復号鍵を有していないため、コンテンツの暗号文7を受信することができたとしても、当然コンテンツの暗号文7を復号することができない。

40

50

【0034】

次に、上記のコンテンツ配信システム1のハードウェア構成について図2を参照して説明する。上記の提供者側サーバ2は、装置全体の制御を行うマイクロプロセッサ20（判別手段）と、各種のデータやプログラム等を格納したハードディスク21と、ハードディスク21に格納された各プログラムの実行時に、各プログラムがローディングされるメモリ22と、各種の指示を入力するためのマウス、キーボード等からなる操作部24と、ユーザ側情報端末3（図1中のユーザ側情報端末3a, 3bに相当）に対するデータの送受信を行う送受信部23（コンテンツ送信手段、ユーザ鍵送信手段）と、ディスプレイ25とを有している。ハードディスク21には、配信用の各種コンテンツ6のデータベースであるコンテンツDB11、コンテンツ7を暗号化するための暗号鍵生成用のプログラムである暗号鍵生成PG12、復号鍵の元になるユーザ鍵を生成するためのプログラムであるユーザ鍵生成PG13、暗号鍵生成PG12で生成された暗号鍵でコンテンツ6（の packets）を暗号化するためのプログラムである暗号化PG14、各種の作業用データ等からなる各種データ15等が格納されている。

10

【0035】

上記のマイクロプロセッサ20及び暗号鍵生成PG12が、請求項における初期値生成手段、カオス系列更新手段、及び暗号鍵生成手段に相当する。また、マイクロプロセッサ20及びユーザ鍵生成PG13が、請求項におけるユーザ鍵生成手段に相当する。さらにまた、マイクロプロセッサ20及び暗号化PG14が、請求項における暗号化手段に相当する。

20

【0036】

また、図に示されるように、ユーザ側情報端末3も、提供者側サーバ2と略同様な構成になっている。ユーザ側情報端末3のハードディスク31には、最新のユーザ鍵に基づいて復号鍵を生成するためのプログラムである復号鍵生成PG16、提供者側サーバ2から送信されたコンテンツの暗号文7を復号するためのプログラムである復号化PG17、その他の作業用データ等からなる各種データ18等が格納されている。ユーザ側情報端末3のその他の構成については、提供者側サーバ2と基本的に同じであるので、ここでは説明を省略する。ユーザ側情報端末3の送受信部33が、請求項における登録要求送信手段、ユーザ鍵受信手段、コンテンツ受信手段、及び証明データ送信手段に相当する。ユーザ側情報端末3のマイクロプロセッサ30及び復号鍵生成PG16が、請求項におけるユーザ鍵更新手段、及び復号鍵生成手段に相当する。ユーザ側情報端末3のマイクロプロセッサ30及び復号化PG17が、請求項における復号手段に相当する。また、ユーザ側情報端末3のマイクロプロセッサ30が、請求項における期限切れ判定手段、及び再登録証明データ生成手段に相当する。

30

【0037】

上記のコンテンツ配信システム1では、カオス写像の特性を利用して、ユーザ鍵（又は復号鍵）に有効期限を設けている。本システム1において利用されているカオス写像の特性には、初期値鋭敏性（初期値依存性）と予測不可能性とがある。初期値鋭敏性とは、カオス系列の初期値における僅かな誤差が、カオス写像を繰り返すことによって、指数関数的に増加するということである。また、予測不可能性とは、カオス系列の正確な初期状態が分からなければ、その振る舞いを予想することができないという性質である。これらの特性のうち、ユーザ鍵に有効期限を設けるのに利用されているのは、主に初期値鋭敏性である。

40

【0038】

具体的には、元のカオス系列の初期値を x 、そのカオス写像を $f(x)$ とすると、元のカオス系列の初期値 x にノイズを加えた値 $(x + \epsilon)$ についてのカオス写像は、 $f(x + \epsilon)$ となる。このとき、初期値 x について1回だけカオス写像をした結果の値である $f(x)$ と、初期値 $(x + \epsilon)$ について1回だけカオス写像をした結果の値である $f(x + \epsilon)$ とは、ほぼ同じ値になる。そして、初期値 x について t 回だけカオス写像をした結果の値である $f^t(x)$ と、初期値 $(x + \epsilon)$ について t 回だけカオス写像をした結果の値

50

である $f^t(x + \epsilon)$ とは、写像回数が少ないときは、ほとんど同じ値を示すが、写像回数が増えると、ノイズが多くなって、全く相関のないような値になる。

【0039】

図3は、下記の(1)式に示されるロジスティック写像(典型的なカオス写像の1つ)を用いて、初期値 $x = 0.12345$ 、ノイズ $\epsilon = 10^{-3}$ とした場合の $f^t(x)$ の値のグラフ41と $f^t(x + \epsilon)$ の値のグラフ42とを示したものである。

$$x_{i+1} = 4x_i(1 - x_i) = f(x_i) \cdots (1)$$

【0040】

図に示されるように、写像の繰り返し回数が少ないときは、これらのグラフ41、42の軌道は限りなく似ているが、多くなると全く異なる軌道となる。

10

【0041】

上記のロジスティック写像は、カオス理論の研究において、おそらく最もよく研究された非線形の動的な系であり、顕著なカオス的特性を有する。ロジスティック写像は、一般的には、下記の非線形差分方程式によって表される一次元の離散時間系である。

$$x_{i+1} = \mu x_i(1 - x_i) \quad (0 < x_i < 1, 0 < \mu < 4)$$

【0042】

本コンテンツ配信システム1では、図3のグラフの作成に使用した $\mu = 4$ の場合のロジスティック写像 $x_{i+1} = 4x_i(1 - x_i)$ を使用する。何故なら、このカオス写像は、完璧なカオス的特性を有し、初期値 x_0 の僅かな差が、将来の値 x_n に大きな差をもたらすからである。

20

【0043】

ロジスティック写像は、10進数の系列を生成するが、10進小数点数の長さは無限であるので、コンピュータ上では、2進数の系列に変換されて計算される。10進数から2進数への変換の演算が行われるとき、近似式が非常に重要となる。もし、カオス系列がTビットの有限の精度で表されるとき、上記の変換は、次の3つの関数のうちの1つによって実現され得る。

$$\text{floor}_T(x) = [x \cdot 2^T] / 2^T \cdots (2)$$

$$\text{round}_T(x) = \text{round}(x \cdot 2^T) / 2^T \cdots (3)$$

$$\text{ceil}_T(x) = \lceil x \cdot 2^T \rceil / 2^T \cdots (4)$$

【0044】

カオス系列がコンピュータで生成されるとき、上記関数の選択を考慮する必要がある。以下の説明では、カオス系列を生成するために、上記3つの式のうちの(3)式を用いる。

30

【0045】

精度と近似のための関数が定義されれば、コンピュータ上において、カオス系列は、独自に生成され得る。そして、このようなデジタルのカオス系列も、初期値鋭敏性を有する。従って、初期値における値の差が極端に小さくても、ロジスティック写像を繰り返すことによって、誤差は累積される。そして、誤差の伝播は、直線的ではない。このことが、カオス軌道を予測不可能にする。

【0046】

ここで、カオス軌道を分析するために、(1)式中の x_i に僅かな誤差を加えて、誤差の伝播について調べる。(1)式より、誤差の伝播は、以下のように表される。

$$\begin{aligned} x_{i+1} + e_{i+1} &= 4(x_i + e_i)(1 - x_i - e_i) \\ &= 4x_i(1 - x_i) + 4e_i(1 - 2x_i - e_i) \end{aligned}$$

【0047】

ここで、 e_i^2 の大きさは、 $e_i(1 - 2x_i)$ よりも遥かに小さいので、無視することができる。従って、下記の式が成立する。

$$x_{i+1} + e_{i+1} \approx 4x_i(1 - x_i) + 4e_i(1 - 2x_i) \cdots (5)$$

【0048】

また、ロジスティック写像の分析において、 $x_i = \sin^2 2^i$ であることが、正確な

40

50

解として知られている。何故なら、

$$\begin{aligned} 4x_i(1-x_i) &= 4\sin^2 2^i (1-\sin^2 2^i) \\ &= 4\sin^2 2^i \cos^2 2^i \\ &= \sin^2 2^{i+1} \\ &= x_{i+1} \cdots (6) \end{aligned}$$

だからである。

【0049】

上記の(5)式と、 $x_i = \sin^2 2^i$ であることより、誤差 e_{i+1} は、下記のように表され得る。

$$\begin{aligned} e_{i+1} &= 4e_i(1-2\sin^2 2^i) \\ &= 4e_i \cos 2^{i+1} \cdots (7) \end{aligned}$$

10

【0050】

上記の検討から、初期値である僅かな誤差 e_0 から伝播した誤差 e_i は、次の式で概算することができる。

【数1】

$$e_i = 4^i e_0 \prod_{t=0}^i \cos 2^t \theta \cdots (8)$$

【0051】

20

上記の(8)式に基づいて、コンピュータで、誤差のビット長を調べると、図4に示されるような結果となった。図4は、ロジスティック写像の繰り返し回数と誤差の(影響のある)ビット長との対応関係を示す。図において、誤差の初期値 e_0 は、 2^{-300} である。コンピュータによるシミュレーション結果から、写像の繰り返し回数に対する誤差の影響のあるビット長の遷移は、直線的であり、図中のグラフの傾きは、概ね1である。それ故、次の仮定を設けることができる。

(仮定1)・・・誤差の影響は、ロジスティック写像を繰り返す度に、より上位の1ビットに伝播していく。

【0052】

本コンテンツ配信システム1では、上記の誤差伝播の性質を利用して、ユーザ鍵の有効期限を調整している。具体的には、共通鍵暗号方式を採用する本コンテンツ配信システム1において、提供者側サーバ2が、 x を初期値とするカオス系列のうちの上位Sビットだけを暗号鍵として用い、ユーザ側情報端末3が、 $(x + e_0)$ を初期値とするカオス系列(ユーザ鍵)のうちの上位Sビットだけを復号鍵として用いるとする。この場合、図5(a)に示されるように、初期状態では、 $(x + e_0)$ を初期値とするユーザ鍵の系列のうち斜線で示される下位kビットのみが、誤差の初期値 e_0 の影響を受けるが、復号鍵として用いられる上位Sビットの部分59は、誤差の初期値 e_0 の影響を受けない。次に、図5(b)に示されるように、 $(x + e_0)$ を初期値として、1回だけロジスティック写像を行うと、上記の(仮定1)より、ロジスティック写像を1回行う度に、誤差の影響が上位の1ビットに伝播していくので、誤差の影響を受ける部分は、斜線で示される下位(k+1)ビットの部分に拡大する。そして、 x を初期値とするカオス系列と $(x + e_0)$ を初期値とするユーザ鍵とにロジスティック写像を繰り返して行うと、ロジスティック写像を繰り返す度に、誤差の影響が上位の1ビットに伝播していくので、図5(c)に示されるように、ロジスティック写像の繰り返し回数が所定の回数を超えると、復号鍵として用いられる上位Sビットの部分59が、誤差の影響を受けるようになってしまう。このことを利用すれば、提供者側とユーザ側とにおいて、一定の期間だけ(有効期限内だけ)鍵の共有を行うことが可能である。

30

40

【0053】

上記のように有効期限内だけ鍵の共有を行うようにするための仕組みについて、下記に説明する。まず、提供者側サーバ2において、カオス系列の初期値 K_0 (図5における初

50

期値 x に相当) を設定する際の処理について説明する。まず、提供者側サーバ 2 は、ビット長 T_s の暗号鍵の初期値 s_k を選択する。そして、この初期値 s_k を用いてロジスティック写像により拡張された暗号鍵の系列が計算される。ここで、注意すべきことは、上記 (1) 式に示されるロジスティック写像の式において、 x_j の範囲は、 $(0 < x_j < 1)$ であるので、上記の暗号鍵の初期値 s_k を、直接、ロジスティック写像に用いることができないということである。暗号鍵の初期値 s_k を、 $(0 \leq x_j < 1)$ の範囲内の 10 進数にするためには、ビットシフト操作が必要である。そして、この s_k に対してビットシフト操作をした結果の数 K_0 が、ロジスティック写像の初期値となる。

【0054】

具体的には、 s_k の 2 進数表現が $\{s_{k_0} s_{k_1} s_{k_2} \cdots s_{k_{T_s-1}}\}$ とすると、ロジスティック写像の初期値 K_0 は、次の式で求められる。 10

【数 2】

$$K_0 = \sum_{j=0}^{T_s-1} s_{k_j} 2^{-(j+1)} \cdots (9)$$

【0055】

上記の初期値 K_0 に基づいて、カオス系列 K_t ($t = 1, 2, 3, \cdots$) が、次のように生成される。

$$K_t = f^t(K_0) \cdots (10)$$

20

【0056】

ロジスティック写像の初期値 K_0 を表現するのに、 T ビットが割り当てられる。ここで、注意すべきことは、 t 番目のカオス系列 K_t も、その時点の初期値となり得るということである。何故なら、 K_t を用いて生成されたカオス系列も、元のカオス系列に付随し、元のカオス系列と同じ性質を維持するからである。例えば、 K_t に僅かな誤差が加えられると、その誤差は、ロジスティック写像を繰り返すことによって、累積される。

【0057】

次に、上記の性質を利用したユーザ鍵の生成方法について説明する。一般に、実際のブロードキャスト型のコンテンツ配信システムでは、ユーザは、自分が興味を持ったときに、ユーザ登録しようとする。従って、提供者側が、ユーザ鍵を何時でも発行することができるのが望ましい。本コンテンツ配信システム 1 では、上記のカオス系列の性質に基づいて、ユーザがユーザ登録を要求したときに、提供者側サーバ 2 が、有効期限付きのユーザ鍵を生成することができる。そのようなユーザ鍵を作るために、その時点の最新のカオス系列 K_t に僅かな誤差を加えてユーザ鍵の初期値とする。カオス系列の特性により、初期値におけるカオス系列 K_t とユーザ鍵 U_t との僅かな誤差のために、元のカオス系列及びユーザ鍵の生成の繰り返しによって引き起こされる、これらの系列の間の誤差は、累積される。そして、ある程度の期間が経過すると(ある程度の回数のロジスティック写像を繰り返すと)、誤差が大きくなり、次の鍵の予測が極めて難しくなる。どの時点のカオス系列 K_t に基づいてユーザ鍵の初期値を生成した場合でも、カオスの特性に基づいて誤差の伝播は生じる。このため、提供者側サーバ 2 は、何時でも、その時点の最新のカオス系列 K_t に基づいてユーザ鍵の初期値を生成することができる。 30 40

【0058】

具体的には、ユーザ側情報端末 3 が、提供者側サーバ 2 にユーザ登録要求のデータを送信すると、提供者側サーバ 2 は、まず、ビット長 T_u の乱数 r を選択する。そして、乱数 r の 2 進数表現 $\{r_0 r_1 r_2 \cdots r_{T_u-1}\}$ を準備する。もし、その時点の最新のカオス系列の系列番号(暗号鍵の更新処理の回数)が t ならば、ユーザ鍵 U_t は、次のように計算される。

【数 3】

$$U_t = K_t + \sum_{j=0}^{T_u-1} r_j 2^{-(T_s+T_p+j+1)} \cdots (11)$$

【0059】

ここで、 T_p は、期間のパラメータであり、 U_t のビット長を T とすると、

$$T = T_s + T_p + T_u \cdots (12)$$

が成立する。

【0060】

上記のユーザ鍵生成のイメージを、図 6 に示す。また、図 7 は、上記(12)式に示される T 、 T_s 、 T_p 、及び T_u の関係を図示したものである。図 7 において、 key と key' とは、それぞれ暗号鍵と復号鍵とを示す。なお、提供者側サーバ 2 における 1 回の暗号鍵の更新処理、及びユーザ側情報端末 3 における 1 回の復号鍵の更新処理では、 n 回のロジスティック写像が行われるため、図において、暗号鍵の元になるカオス系列と復号鍵の元になるユーザ鍵とは、 K_t と U_t とで表されている。

10

【0061】

そして、最終的に、上記の系列番号 t と上記式(11)に示されるユーザ鍵 U_t とが、ユーザ側情報端末 3 に送信される。

【0062】

元のカオス系列 K_t 及びユーザ鍵 U_t のビット長 T は、有効期限をある程度長く確保することができるようにするため、ある程度長くするべきである。また、ビット長 T が一定とすると、提供者側は、乱数 r のビット長 T_u によって有効期限を調整し得る。もし、乱数 r のビット長 T_u が長ければ、有効期限は短く、そして、乱数 r のビット長 T_u が短ければ、有効期限は長い。従って、乱数 r を注意深く選択することによって、有効期限を実際に即した長さに設定することができる。とはいえ、乱数 r のビット長 T_u は、提供者側のカオス系列 K_t についての不正者からの総当り攻撃による分析に対処するために、ある程度以上の長さでなければならない。

20

【0063】

次に、提供者側サーバ 2 とユーザ側情報端末 3 における共通鍵の生成処理について説明する。上述したように、本コンテンツ配信システム 1 におけるカオス系列は、ビット長が T ビットであり、その値は 1 よりも小さい正の 10 進数である。提供者側サーバ 2 とユーザ側情報端末 3 とにおける共通鍵の生成のために、 T ビットのカオス系列から上位 T_s ビットが抽出される。提供者側サーバ 2 は、秘密のカオス系列の初期値 K_0 を用いて、所定の時間が経過する度に、最新のカオス系列の生成を行って、暗号鍵の更新を繰り返す。現在の最新の暗号鍵 key を生成するために、まず、直前のカオス系列 $K_{(t-1)}$ に対してロジスティック写像を n 回繰り返して、最新のカオス系列 K_t を得る。すなわち、

30

$$K_t = f^n(K_{(t-1)}) \cdots (13)$$

の演算を行う。

【0064】

次に、この最新のカオス系列 K_t の上位 T_s ビットを下記の演算により抽出する。

$$key = \text{round}_{T_s}(K_t) \cdots (14)$$

40

【0065】

ここで、関数 $\text{round}_{T_s}(\cdot)$ は、入力値の上位 T_s ビットを出力する関数である。上記のカオス系列 K_t は、初期値 K_0 に基づいて生成されるので、上記の暗号鍵 key は、以下のようにも表される。

$$key = \text{round}_{T_s}(f^t(K_0)) \cdots (15)$$

【0066】

これに対して、ユーザ鍵の初期値 U_t は、その元になるカオス系列 K_t の値と僅かに異なるので、ユーザ鍵の系列は全体的に元のカオス系列と異なる。例えば、ユーザ A のユー

50

ザ鍵の初期値が U_{t_A} であって、その元になるカオス系列が K_{t_A} である場合には、ユーザ側情報端末 3 は、以下のようにユーザ A の復号鍵を求める。

【数 4】

$$key_A = round_{T_s} (f^{at-t_A}(U_{t_A})) \cdots (16)$$

【0067】

ここで、 key_A の有効性は、有効期限に依存している。もし、 $t - t_A$ が T_p (図 7 参照) 以下であれば、 $key = key_A$ となり、 $t - t_A$ が T_p よりも大きければ、 $key = key_A$ とはならない。結局、共通鍵は、有効期間の間、提供者側とユーザとで共有される。 10

【0068】

次に、本コンテンツ配信システム 1 における安全性の分析について述べる。以下の説明では、ユーザに送られたユーザ鍵から提供者のカオス系列を予測することの困難性について述べる。この数十年の間、カオスの分析が続けられているが、数学的な見地から、カオス軌道の予測は難しい。従って、次の仮定を設けることができる。

(仮定 2)・・・カオス系列は、ランダムに分布し、カオス軌道の予測は、初期値が分からなければ困難である。

【0069】

誤差は、ロジスティック写像を繰り返す度に、より上位の 1 ビットに伝播していくので、もし 1 回の更新毎の写像の繰り返し回数が増えると、ユーザ鍵の有効期限は減少する。とはいえ、暗号鍵の生成について考えると、もし 1 回の更新当たりの写像の繰り返し回数が小さいと、悪意のあるユーザが、有効期限が過ぎた後でも、総当たり攻撃によって、現在のユーザ鍵から次のユーザ鍵を予測し得る。例えば、もし、1 回の更新当たりの写像の繰り返し回数が 1 であれば、総当たり攻撃に必要な回数は、わずか 2 回である。何故なら、(仮定 1) より、ユーザ鍵と提供者のカオス系列との相違は、僅か 1 ビットだからである。従って、総当たり攻撃に必要な試行の回数は、2 である。総当たり攻撃に対する防御のために、1 回の更新当たりの写像の繰り返し回数は、複数回である必要がある。また、安全性を考慮すると、写像の繰り返し回数は、大きな数であることが望ましい。 20

【0070】

ここで、本コンテンツ配信システム 1 では、下記の定理が成立する。

(定理 1)・・・有効期限が切れた直後のユーザ鍵 U_t からの有効な共通鍵 key の分析は、 2^{-T_s} の確率で成功する。 30

【0071】

上記の定理の証明は、以下の通りとなる。すなわち、本コンテンツ配信システム 1 では、ビット長 T_s の有効な共通鍵が、秘密鍵暗号システムに基づく暗号通信に用いられる。従って、生成されたカオス系列のうちの上位 T_s ビットだけが、暗号鍵として用いられ、元のカオス系列の残りのビットに関する情報は、鍵共有の操作を行っても、ユーザに漏れない。本コンテンツ配信システム 1 では、カオス系列は、ロジスティック写像により生成される。元のカオス系列 K_t がユーザに漏れると、本コンテンツ配信システム 1 の仕組みは崩壊する。しかし、元のカオス系列 K_t のうちの上位 T_s ビットだけ、すなわち共通鍵のみが、鍵の共有時に、ユーザに漏れるだけである。従って、情報の不足のために、元のカオス系列 K_t の予測は、ユーザにとって困難である。 40

【0072】

ここで、カオス系列の特性から、系列に誤差が含まれていると、その軌道を正確に予測することは困難である。そして、誤差の累積は、避けられない。上位 T_s ビットだけしか漏れないので、攻撃者は、ユーザ鍵 U_t から、元のカオス系列 K_t を分析することはできない。有効な復号鍵が最後に生成された後、ユーザ鍵に基づいて生成された次の復号鍵は、図 8 に示されるように、 T_s ビットの誤差を含む。もし、 T_s が十分に大きければ、復号鍵の分析は困難となる。そして、この場合の総当たり攻撃には、2 回の試行が要求される。 50

それ故、上記の(定理1)は、証明された。

【0073】

本コンテンツ配信システム1の重要な特徴の1つは、ユーザ鍵の有効期限である。(仮定1)と(11)式より、ユーザは、元のカオス系列に近似したユーザ鍵を T_p 回生成することができる。しかし、安全性を考慮すると、全ての(T_p 個の)ユーザ鍵を共通鍵の生成に用いることはできない。ユーザ鍵から抽出された復号鍵の数は、 $T_p /$ でなければならない。

【0074】

ユーザ鍵 U_t の生成において、乱数 r が、その時点の最新のカオス系列 K_t に付加される。その時点の最新のカオス系列 K_t は、常にユーザ鍵の初期値となり得る。従って、ユーザ鍵の生成は、何時でも実行され得る。

10

【0075】

一般に、暗号システムは、秘密鍵が漏れると崩壊し、システムの復旧は、大変困難である。けれども、本コンテンツ配信システム1では、簡単な操作で復旧を行うことができる。秘密鍵が漏れると、提供者側サーバ2は、その時点の最新のカオス系列に乱数を加えることにより、鍵をリフレッシュさせる。この場合、ユーザ鍵の妥当性を保証するために、乱数のビット長は、 T_u にするべきである。システムを復旧するために必要な操作は、上記の操作のみである。安全性の強化のために、提供者側サーバ2が、定期的に、その時点の最新のカオス系列に乱数を加えることが望ましい。

【0076】

次に、図7に示される各パラメータと有効期限の関係について、具体的な数値例を示して説明する。例えば、暗号鍵及び復号鍵のビット長 $T_s = 128$ 、誤差の初期値のビット長 $T_u = 100$ 、カオス系列 K_t 及びユーザ鍵 U_t の1回の更新当たりの写像の繰り返し回数 $= 80$ 、カオス系列 K_t 及びユーザ鍵 U_t の全体のビット長 $T = 2048$ とすると、有効期限は、以下の式で求められる。

20

$$(2048 - 100 - 128) / 80 = 1820 / 80 = 22.75 \text{ (回)}$$

【0077】

従って、カオス系列 K_t 及びユーザ鍵 U_t の更新を1日に1回行うとすれば、ユーザ側と提供者側とは、22日間、鍵の共有を行うことができる。

【0078】

総当たり攻撃に対する耐性を考慮すると、上記のように、カオス系列 K_t 及びユーザ鍵 U_t の1回の更新当たりの写像の繰り返し回数を80回以上に設定することが望ましい。また、この繰り返し回数を総当たり攻撃に耐え得る回数としつつ、ユーザ鍵の有効期限をある程度長い期間に設定するためには、上記のように、カオス系列 K_t 及びユーザ鍵 U_t の全体のビット長 T を2048に設定することが望ましい。

30

【0079】

また、ユーザ毎にユーザ鍵の有効期限を変えることも可能であり、例えば、暗号鍵及び復号鍵のビット長 $T_s = 128$ 、カオス系列 K_t 及びユーザ鍵 U_t の1回の更新当たりの写像の繰り返し回数 $= 80$ 、カオス系列 K_t 及びユーザ鍵 U_t の全体のビット長 $T = 2048$ の場合に、10回分だけ(例えば10日分だけ)ユーザ鍵を(復号鍵を)使えるようにしたい場合には、図7に示される誤差の初期値のビット長 T_u を12回(22回 - 10回)の更新に相当する分だけ埋める(T_u を12回更新後のビット長に設定する)。すなわち、誤差の初期値のビット長 T_u を、

40

$$\{100 + (22 - 10) \times 80\} = 1060$$

に設定する。これにより、有効期限の10回(例えば10日間)が過ぎると、このユーザのユーザ鍵が使用できなくなるようにすることができる。

【0080】

次に、図9及び図10に示されるタイミングチャートと、図11及び図12に示されるフローチャートを参照して、コンテンツ6の暗号文の送受信時とユーザ登録時に、提供者側サーバ2とユーザ側情報端末3において行われる処理について説明する。まず、コンテ

50

コンテンツ6の暗号文の送受信時には、図9に示されるように、提供者側サーバ2は、後述する暗号鍵生成処理(S1)で生成された暗号鍵を用いて、コンテンツ6を暗号化し(S2)、コンテンツ6の暗号文7をユーザ側情報端末3に送信する(S3)。これに対して、ユーザ側情報端末3は、既にユーザ登録済みで、後述する復号鍵生成処理(S4)で生成された復号鍵を既に有している場合には、提供者側サーバ2から送信されたコンテンツ6の暗号文7を受信して(S5)、S4の処理で生成された復号鍵を用いてコンテンツ6の暗号文7を復号する(S6)。

【0081】

また、図10に示されるように、ユーザ登録時に、ユーザ側情報端末3が、提供者側サーバ2にユーザ登録要求のデータを送信すると(S11)、提供者側サーバ2は、このユーザ登録要求のデータを受信して(S12)、その時点の最新のカオス系列に、ユーザ毎の乱数を加算して、ユーザ鍵を生成する(S13)。そして、このユーザ鍵をユーザ側情報端末3に送信する(S14)。ユーザ側情報端末3は、ユーザ鍵を受信すると、このユーザ鍵に基づいて、後述する復号鍵生成処理を行う(S15)。この復号鍵生成処理が終了すると、該当のユーザ側情報端末3では、コンテンツ6の暗号文7を復号することができるようになる。従って、該当のユーザが、コンテンツ6を視聴することができるようになる。

10

【0082】

次に、上記の暗号鍵生成処理について、図11のフローチャートを参照して説明する。最初の暗号鍵の生成時には、提供者側サーバ2は、2進数で表されるカオス系列の初期値を生成し(S21)、このカオス系列の初期値のうちの上位nビット(例えば、128ビット)のみを抽出して、暗号鍵を生成する(S22)。これに対して、2回目以降の暗号鍵の生成処理は、以下のように行われる。提供者側サーバ2は、前回の暗号鍵の生成から所定の時間(例えば、24時間=1日)が経過する度に(S23でYES)、上記(1)式に示されるロジスティック写像を一回(例えば、80回)行って、最新のカオス系列を算出し(S24)、この最新のカオス系列のうちの上位nビットのみを抽出して、暗号鍵を生成するという処理を繰り返す。これにより、所定の時間が経過する度に、暗号鍵が更新される。

20

【0083】

次に、上記の復号鍵生成処理について、図12のフローチャートを参照して説明する。ユーザ側情報端末3は、上記図10中のS13で生成されたユーザ鍵を提供者側サーバ2から受信すると(S31)、受信したユーザ鍵のうちの上位nビット(例えば、128ビット)のみを抽出して、最初の復号鍵を生成する(S32)。これに対して、2回目以降の暗号鍵の生成処理は、以下のように行われる。ユーザ側情報端末3は、提供者側サーバ2から受信したユーザ鍵を初期値として用いて、提供者側サーバ2におけるカオス系列の更新と同じ間隔で(例えば、24時間経過する度に)(S33でYES)、上記(1)式に示されるロジスティック写像を一回行って、最新のユーザ鍵の系列を算出し(S34)、この最新のユーザ鍵の系列のうちの上位nビットのみを抽出して、復号鍵を生成するという処理を繰り返す。これにより、所定の時間が経過する度に、復号鍵が更新される。

30

【0084】

暗号鍵の更新と復号鍵の更新のタイミングを合わせて、ユーザ側の復号鍵を提供者側の暗号鍵と同じ鍵にするために、提供者側は、ユーザ側に、例えば、「毎日12時になったら、暗号鍵を更新するので、それに合わせて復号鍵の更新を行ってほしい」ということを通知しておく。そして、この通知内容に合わせて、提供者側とユーザ側が、毎日12時に暗号鍵の更新処理と復号鍵の更新処理とを行うことにより、ユーザ鍵の有効期限内においては、ユーザ側と提供者側との間で、予備通信を行うことなく、鍵の共有を行うことができる。すなわち、提供者側から見ると、提供者側サーバ2が、ユーザ登録時に、ユーザ側情報端末3にユーザ鍵を送信して、ユーザ登録後は、所定の時間が経過する度に、暗号鍵を更新する処理を行うだけで、ユーザ側情報端末3と予備通信を行うことなく、ユーザとの間で鍵の共有を行うことができ、しかも、ユーザ鍵の発行処理(送信処理)の終了後は

40

50

、ユーザ鍵又は復号鍵の管理をする必要がない。

【0085】

次に、本コンテンツ配信システム1におけるユーザへのコンテンツ配信料金の課金の仕組みについて説明する。本コンテンツ配信システム1では、提供者は、ユーザ登録時にユーザへの課金を行う。すなわち、ユーザは、電子マネーやクレジットカードにより提供者にコンテンツ配信料金を支払った後でなければ、提供者からユーザ鍵を発行してもらえない。ユーザは、ユーザ鍵を発行してもらおうと、このユーザ鍵に基づいて、一定の期間（有効期限）は、提供者側の暗号鍵と同一の鍵（復号鍵）を生成することができるので、提供者側から送信されたコンテンツ6の暗号文7をこの復号鍵で復号することにより、提供者側から送信されたコンテンツ6を視聴することができるようになる。しかし、有効期限が経過すると、ユーザは、再度、ユーザ登録をして、提供者側からユーザ鍵を再発行してもらわなければ、コンテンツ6を視聴することができなくなる。そして、再度ユーザ登録を行うためには、ユーザが、再度、提供者にコンテンツ配信料金を支払う必要がある。従って、提供者側から見ると、ユーザが、所定の時間が経過する度に、再度、ユーザ登録をやり直して、コンテンツ配信料金を支払ってくれるので、提供者が、ユーザに対して正確なコンテンツ配信料金の課金を行うことができる。また、悪意のあるユーザが、ユーザ鍵を不正配布したとしても、一定の期間（有効期限）が経過すると、該当のユーザ鍵を用いて正確な復号鍵を生成することができなくなるので、特にユーザ鍵の管理をする必要がなくなる。

10

【0086】

また、本コンテンツ配信システム1では、2回目以降のユーザ登録時に必要なコンテンツ配信料金を、1回目のユーザ登録時に必要なコンテンツ配信料金より安くすることも容易である。具体的には、ユーザ側情報端末3が、ユーザ鍵の有効期限が切れたときに、有効期限が切れる前に算出されたユーザ鍵のうちの最後に算出されたユーザ鍵に対して、上記(1)式に示されるロジスティック写像を n ($n > 1$) 繰り返して、新たなカオス系列を求めた上で、このカオス系列の上位 n (n は復号鍵のビット長に等しい) ビットを抽出することにより、再登録ユーザであることの証明データを生成する。そして、ユーザ側情報端末3は、ユーザ登録時に提供者側サーバ2から受信したユーザ鍵の初期値と有効期限と共に、上記の証明データを提供者側サーバ2に送信する。この証明データには、ユーザ鍵の初期値に含まれる乱数の影響が現れているので、提供者側サーバ2は、ユーザ側情報端末3から受信したユーザ鍵の初期値と有効期限と証明データとを分析することにより、ユーザ側情報端末3が、ユーザ鍵の初期値に基づいて、本当に該当の証明データを生成することができたか否かを判別することができる。なお、提供者側サーバ2が、ハードディスク21に各ユーザに発行したユーザ鍵の初期値を記録している場合には、ユーザ側情報端末3が、上記の証明データのみを提供者側サーバ2に送信することによって、提供者側サーバ2は、ユーザ側情報端末3が該当の証明データを生成することができたか否かを判別することができる。これにより、過去に登録したことのあるユーザだけに対してコンテンツ配信料金（登録料）の割引を行うようにすることが可能となる。

20

30

【0087】

上述したように、本実施形態によるコンテンツ配信システム1及びそのユーザ鍵管理方法によれば、提供者側サーバ2において最新のカオス系列の算出に用いられるロジスティック写像と、ユーザ側情報端末3において最新のユーザ鍵の算出に用いられるロジスティック写像とは、同じ写像であり、しかも、誤差の伝播のスピードがほぼ一定の写像である。従って、ユーザ鍵の初期値が、その時点の最新のカオス系列に乱数を加算したものであることから、所定の時間経過する度に、最新のカオス系列の値と最新のユーザ鍵の値との誤差が、拡大していく。このため、所定の期間が経過するまでは、最新のカオス系列の上位 n ビットに基づいて生成された暗号鍵と、最新のユーザ鍵の上位 n ビットに基づいて生成された復号鍵とが一致するので、暗号化されたコンテンツを復号することができるが、所定の期間が経過すると、最新のカオス系列の上位 n ビットと最新のユーザ鍵の上位 n ビットとが一致しなくなるため、暗号鍵と復号鍵とが一致しなくなり、暗号化されたコンテ

40

50

ンツを復号することができなくなってしまう。このことは、実質的に、ユーザ鍵に有効期限を設けることと同じである。

【0088】

上記のようにしたことにより、ユーザ登録の期限（ユーザ鍵の有効期限）が切れた場合でも、提供者側サーバ2が、該当ユーザのユーザ側情報端末3との通信等の処理を行って、該当ユーザのユーザ鍵を使用できなくなるようにする必要がなくなる。また、提供者側サーバ2は、その時点の最新のカオス系列に基づき生成した同一の暗号鍵を用いて、全てのユーザ側情報端末3に送信するコンテンツを暗号化することができるので、各ユーザ側情報端末毎に異なるコンテンツの暗号文を送信する必要がなくなる。すなわち、提供者側サーバ2がユーザ管理を行うために必要な処理を、ユーザ登録時におけるユーザ鍵の生成処理だけにすることができる。従って、従来ブロードキャスト暗号システムを採用したブロードキャスト型コンテンツ配信システムと比べて、ユーザ管理に必要なコストの低減を図ることができる。

10

【0089】

また、上記のように、ユーザ鍵に有効期限を設けたことにより、ユーザ鍵の発行から所定の期間が経過すると、ユーザ鍵に基づいて生成される復号鍵が使用できなくなってしまうので、ユーザ鍵が不正に配布された場合でも、その影響を最小限に止めることができる。また、上記のようにユーザ鍵に有効期限を設けたことにより、不正配布者は、ユーザ鍵を非登録ユーザに頻りに配布しなくなれるので、提供者がユーザ鍵の不正配布を検出することができる可能性を高めることができる。すなわち、復号鍵の不正配布問題に有効に対処することができる。

20

【0090】

なお、本発明は、上記実施形態に限られるものではなく、様々な変形が可能である。例えば、上記実施形態では、カオス系列とユーザ鍵の更新に用いるカオス写像を、誤差の伝播のスピードがほぼ一定であるロジスティック写像としたが、カオス系列とユーザ鍵の更新に用いるカオス写像は、これに限られず、誤差の伝播スピードがほぼ一定のカオス写像であればよい。また、図1の説明で付記したように、ユーザ側情報端末をデジタルテレビジョン放送信号受信機とし、提供者側サーバが、暗号化されたコンテンツを、電波によりデジタルテレビジョン放送信号の形式でデジタルテレビジョン放送信号受信機に送信するようにしてもよい。これにより、地上波デジタルテレビジョン放送やBSデジタル放送等の配信システムに本発明を適用することができる。

30

【図面の簡単な説明】

【0091】

【図1】本発明の一実施形態によるブロードキャスト型コンテンツ配信システムにおける処理の概略を示す図。

【図2】上記コンテンツ配信システムのハードウェア構成図。

【図3】上記コンテンツ配信システムに用いられるロジスティック写像を繰り返した場合に、初期値の誤差が与えるカオス系列の値の相違を示すグラフ。

【図4】上記ロジスティック写像の繰り返し回数と誤差のビット長との対応関係を示すグラフ。

40

【図5】(a)(b)(c)は、それぞれ初期状態、上記ロジスティック写像を用いて1回だけ写像を行ったとき、及び同写像を用いてt回写像を行った場合における誤差のビット長を示す図。

【図6】上記コンテンツ配信システムにおけるユーザ鍵生成のイメージを示す図。

【図7】上記コンテンツ配信システムにおけるユーザ鍵の有効期限の説明図。

【図8】上記コンテンツ配信システムにおける安全性の説明図。

【図9】上記コンテンツ配信システムにおけるコンテンツの暗号文の送受信時の処理を示すタイミングチャート。

【図10】上記コンテンツ配信システムにおけるユーザ登録時の処理を示すタイミングチャート。

50

【図11】図9中における暗号鍵生成処理のフローチャート。

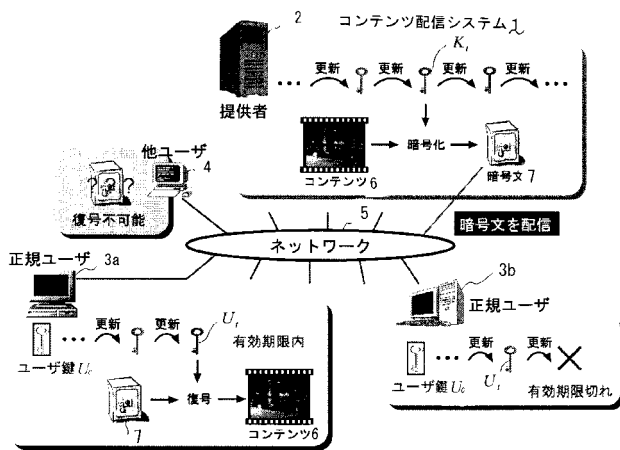
【図12】図9中における復号鍵生成処理のフローチャート。

【符号の説明】

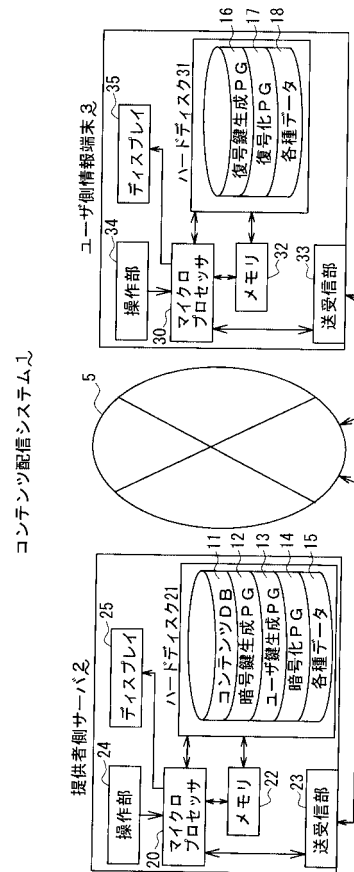
【0092】

- 1 コンテンツ配信システム
- 2 提供者側サーバ（提供者側コンピュータ）
- 3 ユーザ側情報端末
- 5 ネットワーク
- 12 暗号鍵生成PG（初期値生成手段、カオス系列更新手段、暗号鍵生成手段）
- 13 ユーザ鍵生成PG（ユーザ鍵生成手段）
- 14 暗号化PG（暗号化手段）
- 17 復号化PG（復号手段）
- 20 マイクロプロセッサ（ユーザ鍵生成手段、初期値生成手段、カオス系列更新手段、暗号鍵生成手段、暗号化手段、判別手段）
- 23 送受信部（コンテンツ送信手段、ユーザ鍵送信手段）
- 30 マイクロプロセッサ（ユーザ鍵更新手段、復号鍵生成手段、復号手段、期限切れ判定手段、再登録証明データ生成手段）
- 33 送受信部（登録要求送信手段、ユーザ鍵受信手段、コンテンツ受信手段、証明データ送信手段）

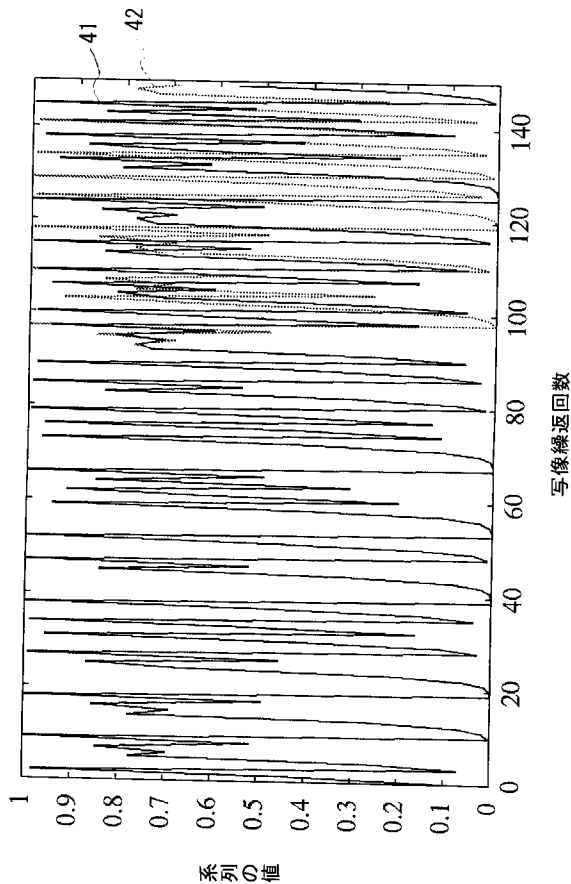
【図1】



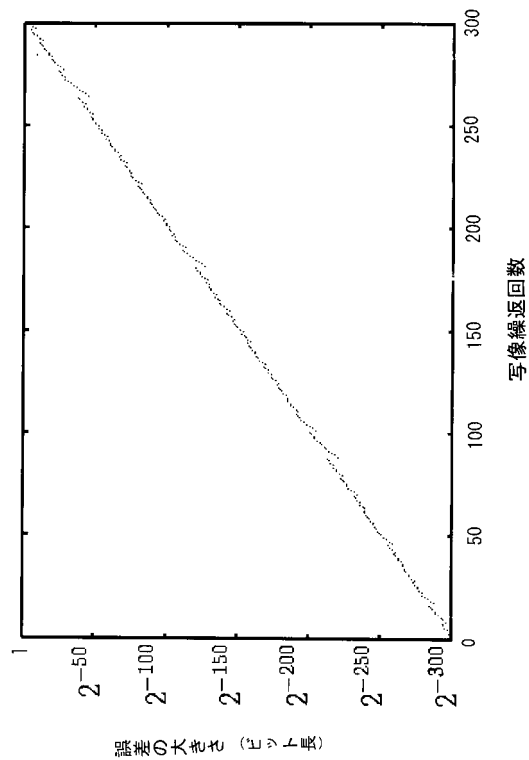
【図2】



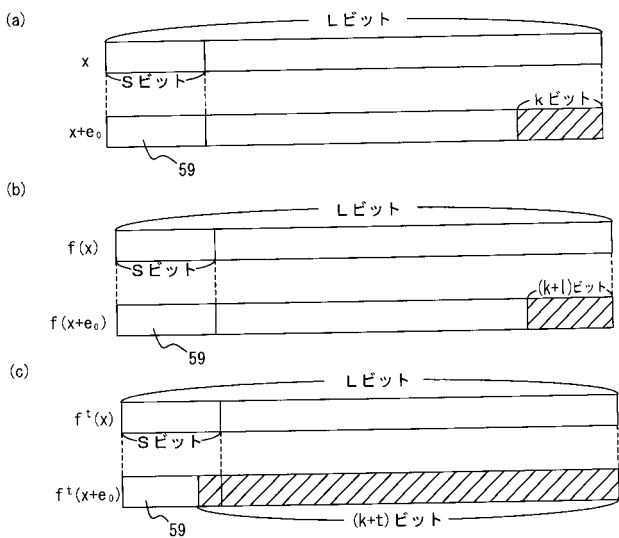
【図3】



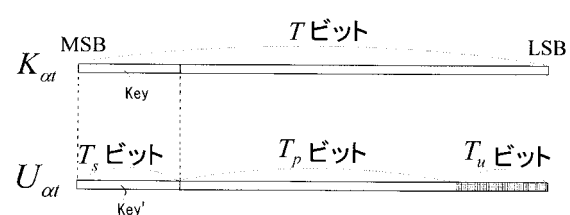
【図4】



【図5】



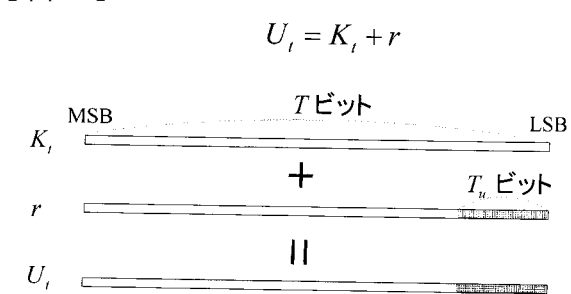
【図7】



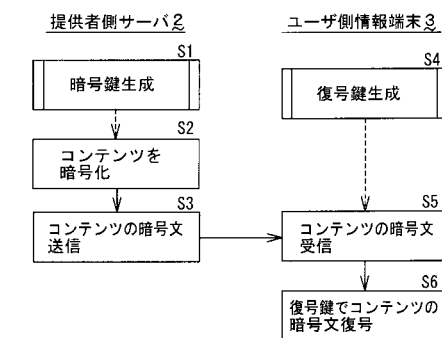
【図8】



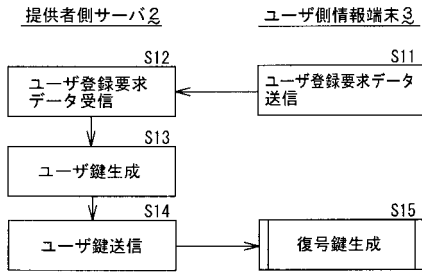
【図6】



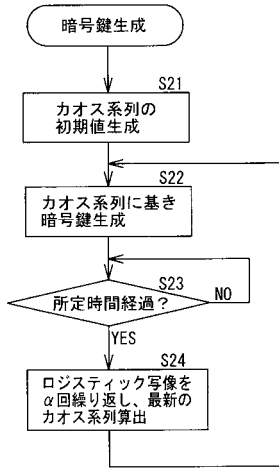
【図9】



【 図 1 0 】



【 図 1 1 】



【 図 1 2 】

