(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4644799号
(P4644799)

(45)発行日　平成23年3月2日(2011.3.2)　(24)登録日　平成22年12月17日(2010.12.17)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04L	9/26	(2006.01)	H04L	9/00	601E
			H04L	9/00	659

請求項の数 14　(全 24 頁)

(21)出願番号　特願2004-380584 (P2004-380584)
(22)出願日　平成16年12月28日 (2004.12.28)
(65)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)
審査請求日　平成19年10月22日 (2007.10.22)

特許法第３０条第１項適用　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

(73)特許権者　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
(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

審査官　松平　英

最終頁に続く

(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)【特許請求の範囲】
【請求項１】
ディ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α回（ただし、α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α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α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α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。

【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β回（ただし、β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、

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。

【請求項７】

前記ユーザ側情報端末は、ディ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、電波によりディジタルテレビジョン放送信号の形式で前記ディ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】

ディ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α回（ただし、α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α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α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】
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β回（ただし、β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、ディ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、電波によりディジタルテ

レビジョン放送信号の形式で前記ディ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、ディ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ため、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。

【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、復号鍵自体か、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
【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。
【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、ディ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α回（ただし、α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α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α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α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β回（ただし、β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、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。

【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、ディ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、電波によりディジタルテレビジョン放送信号の形式で前記ディ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、ディ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α回（ただし、α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α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。

【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αは、１６以上であるものである。

【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β回（ただし、β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ものである。

【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、ディ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、電波によりディジタルテレビジョン放送信号の形式で前記ディ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。

【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することができる。従って、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る。

【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繁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。
【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。
【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αを、１６以上にしたことにより、総当り攻撃に対して、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β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、電波によりディジタルテレビジョン放送信号の形式でディ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、地上波ディジタルテレビジョン放送やＢＳディ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。
【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、ディ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、ディ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をディ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、電波によりディジタルテレビジョン放送信号の形式でディ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。

【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の発行処理だけにすることができる。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。

【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（のパケット）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。

【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。

【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。

【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。

【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εを加えた値（ｘ＋ε）についてのカオス写像は、ｆ（ｘ＋ε）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＋ε）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＋ε）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＋ε）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＋ε）とは、写像回数が少ないときは、ほとんど同じ値を示すが、写像回数が多くなると、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ε＝10^{-30}とした場合のf^t（ｘ）の値のグラフ４１とf^t（ｘ＋ε）の値のグラフ４２とを示したものである。

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

【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。

【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。

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

【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μ＝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。

【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つの関数のうちの一つによって実現され得る。

$floor_T(x)=[x\cdot 2^T]/2^T$・・・（２）

$round_T(x)=round(x\cdot 2^T)/2^T$・・・（３）

$ceil_T(x)=[x\cdot 2^T]/2^T$・・・（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。

【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、このようなディ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。

$$x_{i+1}+e_{i+1}=4(x_i+e_i)(1-x_i-e_i)$$
$$=4x_i(1-x_i)+4e_i(1-2x_i-e_i)$$

【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。

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

【００４８】
また、ロジスティック写像の分析において、$x_i=\sin^2 2^i\theta$であることが、正確な解として知られている。何故なら、

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

だからである。

【００４９】
上記の（５）式と、$x_i=\sin^2 2^i\theta$であることより、誤差e_{i+1}は、下記のように表され得る。

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

【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】

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の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。

【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ｓｋを選択する。そして、この初期値ｓｋ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_iの範囲は、（$0<x_i<1$）であるので、上記の暗号鍵の初期値ｓｋ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ｓｋを、（$0 \leqq x_i \leqq 1$）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ｓｋ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、ｓｋの２進数表現が｛$sk_0\ sk_1\ sk_2 \cdots sk_{T_s-1}$｝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。

【数２】

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

【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，・・・）が、次のように生成される。

$K_t = f^t(K_0)$・・・（１０）

【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。
【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$\{r_0 r_1 r_2 \cdots r_{Tu-1}\}$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、
$T = T_s + T_p + T_u$・・・（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、α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、$K_{\alpha t}$と$U_{\alpha t}$とで表されている。
【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。

【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$K_{\alpha(t-1)}$に対してロジスティック写像をα回繰り返して、最新のカオス系列$K_{\alpha t}$を得る。すなわち、

$K_{\alpha t} = f^{\alpha}(K_{\alpha(t-1)})$ ・・・（１３）

の演算を行う。

【００６４】

次に、この最新のカオス系列$K_{\alpha t}$の上位T_sビットを下記の演算により抽出する。

$key = round_{Ts}(K_{\alpha t})$ ・・・（１４）

【００６５】

ここで、関数$round_{Ts}(\cdot)$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$K_{\alpha t}$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。

$key = round_{Ts}(f^{\alpha t}(K_0))$ ・・・（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のユーザ鍵の初期値がU_{tA}であって、その元になるカオス系列がK_{tA}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】

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

【００６７】

ここで、key_Aの有効性は、有効期限に依存している。もし、$\alpha t - t_A$がT_p（図７参照）以下であれば、$key = key_A$となり、$\alpha t - t_A$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。

【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αが１であれば、総当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、総当り攻撃に必要な試行の回数は、2^{α}である。総当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α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αは、大きな数であることが望ましい。

【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、$2^{-\alpha}$の確率で成功する。

【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。

【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、αビットの誤差を含む。もし、αが十分に大きければ、復号鍵の分析は困難となる。そして、この場合の総当り攻撃には、2^{α}回の試行が要求される。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／α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。

【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$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$の１回の更新当たりの写像の繰り

返し回数α＝８０、カオス系列$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$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。

（２０４８－１００－１２８）／８０＝１８２０／８０＝２２．７５（回）

【００７７】

従って、カオス系列$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$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$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$の１回の更新当たりの写像の繰り返し回数α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αを総当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$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$の全体のビット長Ｔを２０４８に設定することが望ましい。

【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$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$の１回の更新当たりの写像の繰り返し回数α＝８０、カオス系列$K_{\alpha t}$及びユーザ鍵$U_{\alpha t}$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、

｛１００＋（２２－１０）Ｘ８０｝＝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。

【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α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。

【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α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。

【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、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。

【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β回（β＞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。

【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る。

【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繁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。

【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ィ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、電波によりディジタルテレビジョン放送信号の形式でディ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、地上波ディジタルテレビジョン放送やＢＳディ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。

【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。

【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。

【図１１】図９中における暗号鍵生成処理のフローチャート。

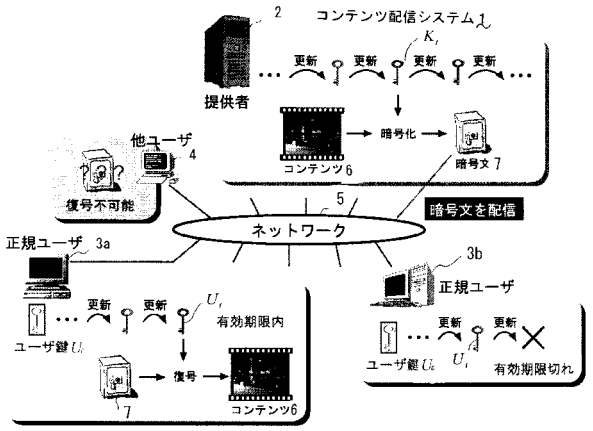
【図１２】図９中における復号鍵生成処理のフローチャート。

【符号の説明】

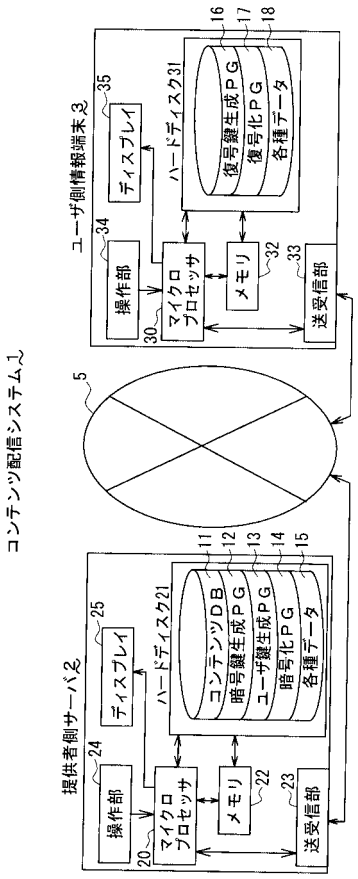
【００９２】

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）

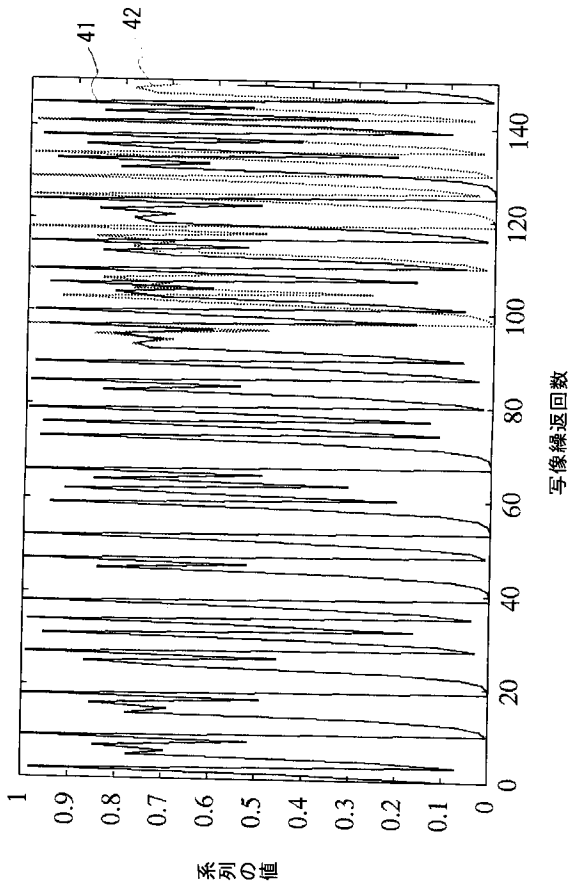
【図１】


コンテンツ配信システム1
提供者
2
更新
暗号化
コンテンツ6
暗号文7
他ユーザ
4
復号不可能
ネットワーク
5
暗号文を配信
正規ユーザ 3a
3b
正規ユーザ
有効期限内
復号
ユーザ鍵
有効期限切れ

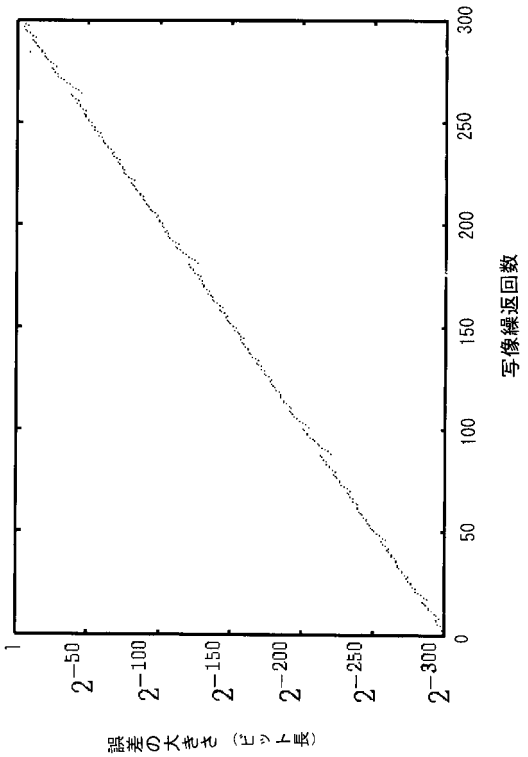
【図２】


コンテンツ配信システム1
ユーザ側情報端末3
提供者側サーバ2
ディスプレイ
ハードディスク31
操作部
マイクロプロセッサ
メモリ
送受信部
コンテンツDB
暗号鍵生成PG
ユーザ鍵生成PG
暗号化PG
各種データ
復号鍵生成PG
復号化PG

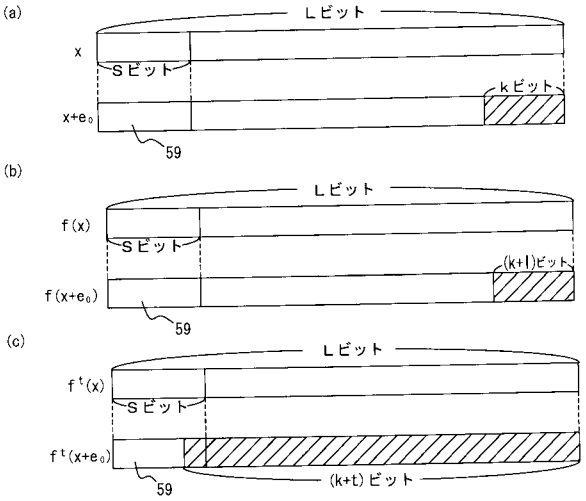
【図３】


41
42
系列の値
写像繰返回数

【図４】

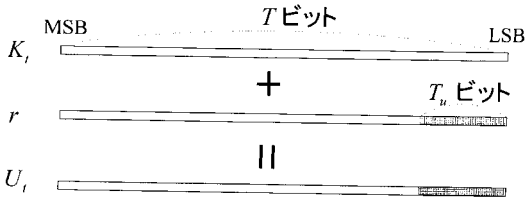

誤差の大きさ（ビット長）
写像繰返回数

【図５】

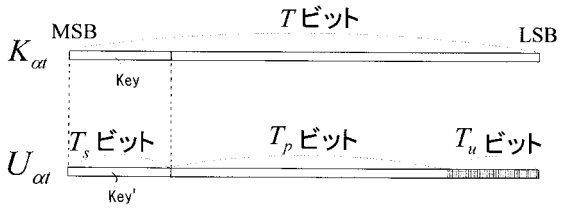


【図６】

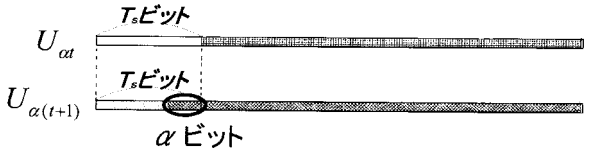
$$U_t = K_t + r$$



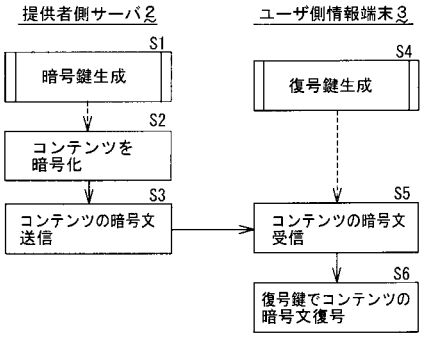
【図７】



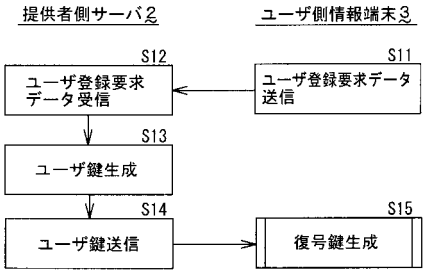
【図８】



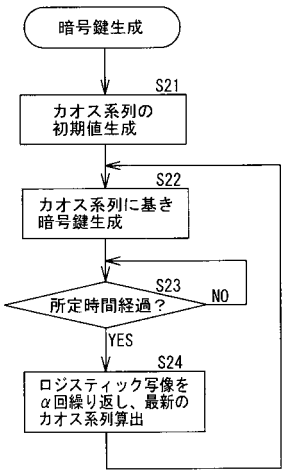
【図９】



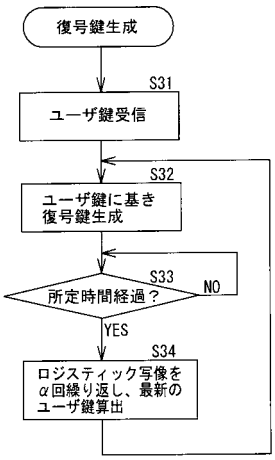
【図１０】



【図１１】



【図１２】



フロントページの続き

(56)参考文献 特開２００１－２８５２７９（ＪＰ，Ａ）
特開２００１－２８５２７７（ＪＰ，Ａ）
特開２００３－１５２７０６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００
Ｇ０９Ｃ　　１／００
Ｈ０４Ｎ　　７／１６
Ｈ０４Ｈ　２０／００