(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4701381号
(P4701381)
(45)発行日　平成23年6月15日(2011.6.15)　(24)登録日　平成23年3月18日(2011.3.18)

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

請求項の数 11　(全 21 頁)

(21)出願番号　特願2005-16142(P2005-16142)
(22)出願日　平成17年1月24日(2005.1.24)
(65)公開番号　特開2006-203824(P2006-203824A)
(43)公開日　平成18年8月3日(2006.8.3)
審査請求日　平成19年12月18日(2007.12.18)

(73)特許権者　504143441
国立大学法人　奈良先端科学技術大学院大学
奈良県生駒市高山町８９１６－５
(74)代理人　110000338
特許業務法人原謙三国際特許事務所
(72)発明者　楫　勇一
奈良県生駒市高山町８９１６－５大学宿舎Ｂ－２０５

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号鍵生成装置、暗号鍵生成方法、暗号化データ配信装置、個別暗号鍵再生成装置、暗号化データ受信装置、暗号化データ配信システム、暗号鍵生成プログラム、および記録媒体

(57)【特許請求の範囲】
【請求項１】
一般に公開する、可換な第１および第２落とし戸付き一方向性置換と、
上記第１落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第１一方向性逆置換と、
上記第２落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第２一方向性逆置換とを用いて暗号鍵を生成する暗号鍵生成装置であって、
所定の初期暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とをそれぞれ適用することによって、入力データの暗号化および復号化に用いられる、複数の互いに異なる個別暗号鍵を生成する個別暗号鍵生成手段と、
上記個別暗号鍵生成手段によって生成される上記複数の個別暗号鍵のいずれかに、上記第１および第２一方向性逆置換の少なくとも一方を、少なくとも１回適用することによって、上記個別暗号鍵の再生成に用いられるマスタ暗号鍵を生成するマスタ暗号鍵生成手段とを備えていることを特徴とする暗号鍵生成装置。
【請求項２】
上記第１および第２落とし戸付き一方向性置換は、ＲＳＡ関数であることを特徴とする請求項１に記載の暗号鍵生成装置。
【請求項３】
上記第１および第２落とし戸付き一方向性置換は、直交一方向性を満たしていることを

特徴とする請求項１に記載の暗号鍵生成装置。
【請求項４】
上記個別暗号鍵生成手段は、生成した上記個別暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とを適用することによって、異なる新たな個別暗号鍵を生成することを特徴とする請求項１に記載の暗号鍵生成装置。
【請求項５】
請求項１に記載の暗号鍵生成装置によって生成された複数の各個別暗号鍵を用いて、複数の配信用データをそれぞれ暗号化することによって、暗号化データを生成する暗号化データ生成手段と、
上記暗号化データを、通信ネットワークを通じて暗号化データ受信装置に配信する暗号化データ配信手段と、
を備えていることを特徴とする暗号化データ配信装置。
【請求項６】
請求項１に記載の暗号鍵生成装置によって生成された上記マスタ暗号鍵の入力を受け付けるマスタ暗号鍵入力手段と、
上記入力されたマスタ暗号鍵に上記第１落とし戸付き一方向性置換および第２落とし戸付き一方向性置換の少なくともいずれかを適用することによって、請求項１に記載の暗号鍵生成装置によって生成された複数の個別暗号鍵のうち一部を再生成する個別暗号鍵再生成手段を備えていることを特徴とする個別暗号鍵再生成装置。
【請求項７】
請求項６に記載の個別暗号鍵再生成装置によって生成された個別暗号鍵の入力を受け付ける個別暗号鍵入力手段と、
請求項５に記載の暗号化データ配信装置によって配信された上記暗号化データを受信する暗号化データ受信手段と、
入力された上記個別暗号鍵を用いて、上記受信した暗号化データを復号化する配信データ復号化手段とを備えていることを特徴とする暗号化データ受信装置。
【請求項８】
請求項５に記載の暗号化データ配信装置と、請求項７に記載の暗号化データ受信装置とを含んでいる暗号化データ配信システム。
【請求項９】
一般に公開する、可換な第１および第２落とし戸付き一方向性置換と、
上記第１落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第１一方向性逆置換と、
上記第２落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第２一方向性逆置換とを用いて、請求項１～４のいずれか１項に記載の暗号鍵生成装置が暗号鍵を生成する暗号鍵生成方法であって、
上記個別暗号鍵生成手段が、所定の初期暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とをそれぞれ適用することによって、入力データの暗号化に用いられる複数の互いに異なる個別暗号鍵を生成する個別暗号鍵生成工程と、
上記マスタ暗号鍵生成手段が、生成された上記複数の個別暗号鍵のいずれかに、上記第１および第２一方向性逆置換の少なくとも一方を、少なくとも１回適用することによって、マスタ暗号鍵を生成するマスタ暗号鍵生成工程とを含んでいることを特徴とする暗号鍵生成方法。
【請求項１０】
請求項１～４のいずれかに記載の暗号鍵生成装置を動作させる暗号鍵生成プログラムであって、コンピュータを上記の各手段として機能させるための暗号鍵生成プログラム。
【請求項１１】
請求項１０に記載の暗号鍵生成プログラムを格納しているコンピュータ読み取り可能な

記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、あらかじめ決められた特定の暗号化データを復号可能な暗号鍵を生成する技術に関する。
【背景技術】
【０００２】
今日、数多くの情報関連サービスにおいて、暗号文（暗号化データ）を解読（復号化）するために必要な暗号鍵を、正当なユーザにのみ配布することによって、第三者や不正なユーザによる、サービスの不正な利用を防止する技術が知られている。このような技術を利用して、たとえば、通信ネットワークや放送型通信路を介して、映画等のコンテンツを有料で配信するサービスや、無線ＬＡＮ等のネットワーク資源を有料で提供するサービスなどがユーザに提供されている。
【０００３】
一方で、ユーザは、指定した一定時間、すなわち限定された特定の時間帯においてのみ、情報の提供を受けられるような、時間限定型のサービスを求めている。このようなサービスとして、たとえば、１時間だけ視聴可能な有料テレビ放送や、３０分だけ使用可能な無線ＬＡＮサービスなどが考えられる。
【０００４】
このような要請に対応すべく、時間限定型の情報提供サービスを実現するための暗号鍵方式が、非特許文献１および２において提案されている。非特許文献１には、ロジスティック写像の振る舞いを利用することによって、時間限定で鍵更新に追従する方法が開示されている。非特許文献２には、コンテンツの特定区間だけを復号可能とする暗号鍵の派生方式が開示されている。
【非特許文献１】M. Kuribayashi and H. Tanaka: "A New Key Generation Method for Broadcasting System with Expiration Date," 27th Symp. on Information Theory and Its Appications (SITA2004), pp. 323-326 (2004)
【非特許文献２】須賀、岩村：”一次元コンテンツにおけるアクセス制御のための鍵派生方式”、コンピュータセキュリティシンポジウム２００４（css2004）、pp.481-486 (2004)
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、これらの特許文献において提案されている方法は、未だ、実用的なレベルに到達していない。たとえば、復号化を限定できる時間やデータの数に制限があるなど、暗号鍵生成の効率や柔軟性が不十分である。
【０００６】
本発明は上記の課題を解決するためになされたものであり、その目的は、入力データの暗号化および復号化に用いられる複数の個別暗号鍵、および、個別暗号鍵の一部のみを再生成可能なマスタ暗号鍵を効率的かつ柔軟に生成する暗号鍵生成装置、暗号鍵生成方法、暗号鍵生成プログラム、およびこの暗号鍵生成プログラムを記録しているコンピュータ読み取り可能な記録媒体を提供することにある。
【０００７】
さらに、本発明の第２の目的は、このような暗号鍵生成装置によって生成された個別暗号鍵を用いて、入力データを暗号化し、暗号化データ受信装置に配信する暗号化データ配信装置を提供することにある。
【０００８】
さらに、本発明の第３の目的は、上述した暗号鍵生成装置によって生成されたマスタ暗号鍵を用いて、個別暗号鍵を再生成する個別暗号鍵再生成装置を提供することにある。

【０００９】
さらに、本発明の第４の目的は、上述した暗号化データ配信装置によって配信された暗号化データを受信し、マスタ暗号鍵を用いて個別暗号鍵を再生成し、当該再生成した個別暗号鍵を用いて、受信した一部の暗号化データを復号化する暗号化データ受信装置を提供することにある。
【００１０】
さらに、本発明の第５の目的は、上述した暗号化データ配信装置および暗号化データ受信装置からなる暗号化データ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】
【００１１】
上記の課題を解決するために、本発明に係る暗号鍵生成装置は、一般に公開する、可換な第１および第２落とし戸付き一方向性置換と、上記第１落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第１一方向性逆置換と、上記第２落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第２一方向性逆置換とを用いて暗号鍵を生成する暗号鍵生成装置であって、所定の初期暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とをそれぞれ適用することによって、入力データの暗号化および復号化に用いられる、複数の互いに異なる個別暗号鍵を生成する個別暗号鍵生成手段と、上記個別暗号鍵生成手段によって生成される上記複数の個別暗号鍵のいずれかに、上記第１および第２一方向性逆置換の少なくとも一方を、少なくとも１回適用することによって、上記個別暗号鍵の再生成に用いられるマスタ暗号鍵を生成するマスタ暗号鍵生成手段とを備えていることを特徴としている。
【００１２】
本発明の暗号鍵生成装置は、公開鍵暗号方式に基づき、個別暗号鍵およびマスタ暗号鍵を生成する。具体的には、暗号鍵生成装置は、一般に公開する、可換な第１および第２落とし戸付き一方向性置換と、上記第１落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第１一方向性逆置換と、上記第２落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第２一方向性逆置換とを用いることによって、暗号鍵を生成する。
【００１３】
ここで、「可換」とは、同一回数の第１落とし戸付き一方向性置換と同一回数の第２落とし戸付き一方向性置換を同一の入力データに適用した場合、適用する第１および第２落とし戸付き一方向性置換の順序に関係なく、同一の出力データが得られる条件が成立することを意味する。すなわち、暗号鍵生成装置では、ある入力データに１回の第１落とし戸付き一方向性置換を適用し、次に１回の第２落とし戸付き一方向性置換を適用して得られる出力データと、同じ入力データに１回の第２落とし戸付き一方向性置換を適用し、次に１回の第１落とし戸付き一方向性置換を適用して得られる出力データとは、同一の値を取る。
【００１４】
上述した第１一方向性逆置換は、第１落とし戸付き一方向性置換の逆置換である。これにより、暗号鍵生成装置では、ある入力データに第１落とし戸付き一方向性置換を適用して得られる出力データに、さらに、第１一方向性逆置換を適用すると、もとの入力データが得られる。このことは、第２落とし戸付き一方向性置換と第２一方向性逆置換との関係においても、同様である。すなわち、上述した第２一方向性逆置換は、第２落とし戸付き一方向性置換の逆置換である。これにより、暗号鍵生成装置では、ある入力データに第２落とし戸付き一方向性置換を適用して得られる出力データに、さらに、第２一方向性逆置換を適用すると、もとの入力データが得られる。
【００１５】
なお、暗号鍵生成装置は、第１落とし戸付き一方向性置換と可換であるが同一でない第２落とし戸付き一方向性置換を用いる。これにより、第１および第２落とし戸付き一方向性置換を用いて生成される個別暗号鍵が、全て同一の値を取ることを防止できる。また、

一般に、第１落とし戸付き一方向性置換と第１一方向性逆置換も、可換である。しかし、暗号鍵生成装置は、第２落とし戸付き一方向性置換として第１一方向性逆置換を用いることはない。すなわち、暗号鍵生成装置は、第１一方向性逆置換とは異なる第２落とし戸付き一方向性置換を用いる。これによっても、第１および第２落とし戸付き一方向性置換を用いて生成される個別暗号鍵が、全て同一の値を取ることを防止できる。

【００１６】

上記の構成によれば、個別暗号鍵生成手段は、互いに異なる複数の個別暗号鍵を生成する。このとき生成される複数の個別暗号鍵では、第１および第２一方向性逆置換の少なくとも一方を適用しない限り、ある個別暗号鍵から、別の個別暗号鍵を再生成できない。一方、マスタ暗号鍵生成手段は、このような複数の個別暗号鍵のうち、いずれか１つの個別暗号鍵に、第１および第２一方向性逆置換の少なくとも一方を、少なくとも１回適用することによって、個別暗号鍵の再生成に用いられるマスタ暗号鍵を生成する。

【００１７】

ここで、一般に、公開されている第１落とし戸付き一方向性置換に基づき、非公開の第１一方向性逆置換を導出することは、極めて困難である。第１一方向性逆置換と同様に、非公開の第２一方向性逆置換も、公開されている第２落とし戸付き一方向性置換から導出することは、極めて困難である。入力されたマスタ暗号鍵を用いて個別暗号鍵を再生成する個別暗号鍵再生成装置は、マスタ暗号鍵に、一般に公開されている第１および第２落とし戸付き一方向性置換を適用できるが、一般に非公開にされている第１および第２一方向性逆置換を適用することはできない。

【００１８】

これにより、いったん生成されたマスタ暗号鍵には、第１一方向性逆置換や第２一方向性逆置換を適用することができない。すなわち、第１一方向性逆置換や第２一方向性逆置換を適用しないと生成できない個別暗号鍵を、いったん生成されたマスタ暗号鍵から、再生成することはできない。

【００１９】

一方、個別暗号鍵生成手段によって生成される、互いに異なる複数の個別暗号鍵では、第１および第２一方向性逆置換の少なくとも一方を適用しない限り、ある個別暗号鍵から、別の個別暗号鍵を再生成できない。そのため、いったん生成されたマスタ暗号鍵からは、個別暗号鍵生成手段によって生成される個別暗号鍵のうち、一部のみを再生成できることになる。

【００２０】

すなわち、マスタ暗号鍵生成手段は、複数の個別暗号鍵のうち、一部のみを再生成可能なマスタ暗号鍵を生成する。このとき、マスタ暗号鍵生成手段は、個別暗号鍵に適用する第１一方向性逆置換または第１一方向性逆置換、あるいはこれらの両方の回数を多くするほど、再生成できる個別暗号鍵の範囲がより広いマスタ暗号鍵を生成できる。

【００２１】

以上のように、本装置は、入力データの暗号化および復号化に用いられる複数の個別暗号鍵、および、個別暗号鍵の一部のみを再生成可能なマスタ暗号鍵を、効率的かつ柔軟に生成できる効果を奏する。

【００２２】

上記の課題を解決するために、本発明に係る暗号鍵生成方法は、一般に公開する、可換な第１および第２落とし戸付き一方向性置換と、上記第１落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第１一方向性逆置換と、上記第２落とし戸付き一方向性置換の逆置換であり、かつ、一般に非公開にする第２一方向性逆置換とを用いて暗号鍵を生成する暗号鍵生成方法であって、所定の初期暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とをそれぞれ適用することによって、入力データの暗号化に用いられる複数の互いに異なる個別暗号鍵を生成する個別暗号鍵生成工程と、生成された上記複数の個別暗号鍵のいずれかに、上記第１および第２一方向性逆置換の少なくとも一方を、少なくとも１回適用することによっ

て、マスタ暗号鍵を生成するマスタ暗号鍵生成工程とを含んでいることを特徴としている。

【００２３】

上記の構成によれば、上述した暗号鍵生成装置と同様の作用、効果を奏する。

【００２４】

また、本発明の暗号鍵生成装置では、上記第１および第２落とし戸付き一方向性置換は、ＲＳＡ関数であることが好ましい。

【００２５】

上記の構成によれば、暗号鍵生成装置を、広く流通しているＲＳＡ関数を用いた構成とすることができる。これにより、実用的な暗号強度を有する個別暗号鍵およびマスタ暗号鍵を生成できる効果を奏する。

【００２６】

また、本発明の暗号鍵生成装置では、上記第１および第２落とし戸付き一方向性置換は、直交一方向性を満たしていることが好ましい。

【００２７】

上記の構成によれば、これにより、一般に公開する第１および第２落とし戸付き一方向性置換から、落とし戸情報を知らずに第１および第２一方向性逆置換を導出できる可能性が、より低くなる。したがって、個別暗号鍵およびマスタ暗号鍵の秘匿性をより高めることができる効果を奏する。

【００２８】

また、本発明の暗号鍵生成装置では、上記個別暗号鍵生成手段は、生成した上記個別暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とを適用することによって、異なる新たな個別暗号鍵を生成することが好ましい。

【００２９】

上記の構成によれば、個別暗号鍵生成手段は、生成した個別暗号鍵を新たな入力データとして、新たな個別暗号鍵を再帰的に生成する。したがって、暗号鍵生成装置は、複数の互いに異なる個別暗号鍵を、より効率的に生成できる効果を奏する。

【００３０】

上記の課題を解決するために、本発明に係る暗号化データ配信装置は、上述した暗号鍵生成装置によって生成された複数の各個別暗号鍵を用いて、複数の配信用データをそれぞれ暗号化することによって、暗号化データを生成する暗号化データ生成手段と、上記暗号化データを、通信ネットワークを通じて暗号化データ受信装置に配信する暗号化データ配信手段と、を備えていることを特徴としている。

【００３１】

上記の構成によれば、暗号化データ配信装置は、個別暗号鍵を用いて暗号化した入力データを、暗号化データとして、暗号化データ受信装置に配信する。すなわち、一部のみを復号化できる暗号化データを配信できる暗号化データ配信装置を提供できる効果を奏する。

【００３２】

上記の課題を解決するために、本発明に係る個別暗号鍵再生成装置は、上述した暗号鍵生成装置によって生成された上記マスタ暗号鍵の入力を受け付けるマスタ暗号鍵入力手段と、上記入力されたマスタ暗号鍵に上記第１落とし戸付き一方向性置換および第２落とし戸付き一方向性置換の少なくともいずれかを適用することによって、上述した暗号鍵生成装置によって生成された個別暗号鍵を再生成する個別暗号鍵再生成手段を備えていることを特徴としている。

【００３３】

上記の構成によれば、個別暗号鍵再生成装置において、暗号鍵生成装置によって生成されたマスタ暗号鍵に基づき、個別暗号鍵が再生成される。上述したように、マスタ暗号鍵からは、暗号鍵生成装置によって生成された複数の個別暗号鍵のうち一部のみが再生成さ

れる。このため、暗号鍵生成装置によって生成された複数の個別暗号鍵のうち、一部のみを再生成する個別暗号鍵再生成装置を提供できる効果を奏する。

【００３４】

上記の課題を解決するために、本発明に係る暗号化データ受信装置は、上述した個別暗号鍵再生成装置によって生成された個別暗号鍵の入力を受け付ける個別暗号鍵入力手段と、上述した暗号化データ配信装置によって配信された上記暗号化データを受信する暗号化データ受信手段と、入力された上記個別暗号鍵を用いて、上記受信した暗号化データを復号化する配信データ復号化手段とを備えていることを特徴としている。

【００３５】

上記の構成によれば、配信された暗号化データのうち、事前に復号化可能に設定されている一部の暗号化データのみを復号化する暗号化データ受信装置を提供できる効果を奏する。

【００３６】

上記の課題を解決するために、本発明に係る暗号化データ配信システムは、上述した暗号化データ配信装置および暗号化データ受信装置を含んでいることを特徴としている。

【００３７】

上記の構成によれば、配信された暗号化データのうち、事前に復号化可能に設定されている一部の暗号化データのみを復号化する暗号化データ配信システムを提供できる効果を奏する。

【００３８】

なお、上記暗号鍵生成装置は、コンピュータによって実現してもよい。この場合、コンピュータを上記各手段として動作させることにより上記暗号鍵生成装置をコンピュータにて実現させる暗号鍵生成プログラム、およびその暗号鍵生成プログラムを記録したコンピュータ読み取り可能な記録媒体も、本発明の範疇に入る。

【発明の効果】

【００３９】

以上のように、本発明に係る暗号鍵生成装置は、所定の初期暗号鍵に、少なくとも１回の上記第１一方向性逆置換と、少なくとも１回の上記第２落とし戸付き一方向性置換とをそれぞれ適用することによって、入力データの暗号化に用いられる複数の互いに異なる個別暗号鍵を生成する個別暗号鍵生成手段と、上記個別暗号鍵生成手段によって生成される上記複数の個別暗号鍵のいずれかに、上記第１および第２一方向性逆置換の少なくとも一方を、少なくとも１回適用することによって、マスタ暗号鍵を生成するマスタ暗号鍵生成手段とを備えているため、入力データの暗号化および復号化に用いられる複数の個別暗号鍵、および、個別暗号鍵の一部のみを再生成可能なマスタ暗号鍵を効率的かつ柔軟に生成できる効果を奏する。

【発明を実施するための最良の形態】

【００４０】

本発明の一実施形態について、図１～図３を参照して以下に説明する。

【００４１】

まず、図２を参照して、本発明に係る暗号化データ配信システム１の概略を説明する。

【００４２】

図２は、本発明に係る暗号化データ配信システム１の詳細な構成を示すブロック図である。図２に示す暗号化データ配信システム１は、暗号化データ配信装置１０と暗号化データ受信装置３０からなるシステムである。すなわち、暗号化データ配信システム１では、暗号化データ配信装置１０と暗号化データ受信装置３０との間において、暗号化データのやり取りが行われる。

【００４３】

図２に示すように、暗号化データ配信装置１０は、暗号鍵生成装置２０を備えている。暗号鍵生成装置２０は、公開鍵暗号方式に基づき、スクランブル鍵（個別暗号鍵）および時限鍵（マスタ暗号鍵）を生成する。この詳細については、後述する。暗号鍵生成装置２

０は、生成したスクランブル鍵を、暗号化データ配信装置１０に提供する。暗号化データ配信装置１０は、暗号鍵生成装置２０によって生成されたスクランブル鍵を用いて、入力された配信データを暗号化する。これによって、暗号化データ配信装置１０は、上記スクランブル鍵によって復号化できる暗号化データを生成する。

【００４４】

暗号化データ配信装置１０は、生成した暗号化データを、通信ネットワークを介して暗号化データ受信装置３０に配信する。同時に、暗号化データ配信装置１０は、暗号鍵生成装置２０によって生成された時限鍵を、暗号化データ受信装置３０に配信する。すなわち、暗号化データ配信装置１０は、暗号化された配信データを暗号化データ受信装置３０に配信すると共に、配信した暗号化データを配信データに復号化するために必要なスクランブル鍵を導出（再生成）するための時限鍵をも、暗号化データ受信装置３０に配信する。

【００４５】

暗号化データ受信装置３０は、通信ネットワークを通じて配信された暗号化データおよび時限鍵を受信する。受信した時限鍵に基づき、暗号化データ受信装置３０は、配信データの暗号化に使用されたスクランブル鍵を再生成する。再生成したスクランブル鍵を用いて、暗号化データ受信装置３０は、暗号化データを復号化する。これにより、暗号化データ受信装置３０は、配信された暗号化データから、元の配信データを生成する。すなわち、暗号化データ受信装置３０は、配信データを復元する。

【００４６】

このようにして、暗号化データ配信システム１では、暗号化データ配信装置１０と暗号化データ受信装置３０との間において、暗号化データのやり取りが行われる。後述するように、暗号化データ配信システム１では、暗号化データ受信装置３０において復号化可能な暗号化データは、あらかじめ定められた（暗号化データ受信装置３０が設定した）一部のみである。すなわち、暗号化データ配信システム１において、暗号鍵生成装置２０は、スクランブル放送に適用可能な、短時間で次々と新しいスクランブル鍵に更新可能なスクランブル鍵を生成する。また、生成されるスクランブル鍵のうち、特定の一部のみを再生成可能な時限鍵を、同時に生成する。

【００４７】

暗号鍵生成装置２０は、配信データの暗号化に用いられるスクランブル鍵のうち、再生成可能な範囲が事前に柔軟に設定されている時限鍵を生成する。したがって、時限鍵を用いてスクランブル鍵を再生成するスクランブル鍵再生成部３３は、スクランブル鍵のうち、事前に設定されている一部のスクランブル鍵のみを再生成できる。すなわち、暗号化データ受信装置３０は、再生成されたスクランブル鍵を用いて、受信した暗号化データの一部のみを復号化する。これにより、暗号化データ配信システム１において、配信されるデータの一部利用が実現できる。

【００４８】

暗号鍵生成装置２０は、以上のようなスクランブル鍵および時限鍵を、公開鍵暗号方式に基づいて生成する。また、スクランブル鍵再生成部３３も、暗号鍵生成装置２０が利用する公開鍵暗号方式に基づいて、時限鍵からスクランブル鍵を再生成する。そこで、本発明の暗号鍵生成装置２０およびスクランブル鍵再生成部３３について、以下に詳細に説明する。

【００４９】

まず、暗号鍵生成装置２０について、図１を参照して以下に詳細に説明する。図１は、本発明に係る暗号鍵生成装置２０の構成を詳細に示すブロック図である。この図に示すように、暗号鍵生成装置２０は、初期鍵データベース２２、置換関数データベース２４、スクランブル鍵生成部２６、および時限鍵生成部２８を備えている。

【００５０】

上述したように、暗号鍵生成装置２０は、公開鍵暗号方式に基づき、暗号鍵を生成する。具体的には、暗号鍵生成装置２０は、一般に公開する、可換な落とし戸付き一方向性置換h_1およびh_2と、落とし戸付き一方向性置換h_1の逆置換であり、かつ、一般に非公

開にする一方向性逆置換h_1^{-1}と、落とし戸付き一方向性置換h_2の逆置換であり、かつ、一般に非公開にする一方向性逆置換h_2^{-1}とを用いることによって、暗号鍵を生成する。

【００５１】

ここで、「可換」とは、同一回数の落とし戸付き一方向性置換h_1と同一回数の落とし戸付き一方向性置換h_2を同一の入力データに適用した場合、入力データに適用する落とし戸付き一方向性置換h_1およびh_2の順序に関係なく、同一の出力データが得られる条件が成立することを意味する。すなわち、暗号鍵生成装置２０では、ある入力データに１回の落とし戸付き一方向性置換h_1を適用し、次に１回の落とし戸付き一方向性置換h_2を適用して得られる出力データと、同じ入力データに１回の落とし戸付き一方向性置換h_2を適用し、次に１回の落とし戸付き一方向性置換h_1を適用して得られる出力データとは、同一の値を取る。

【００５２】

一方向性逆置換h_1^{-1}は、落とし戸付き一方向性置換h_1の逆置換である。これにより、暗号鍵生成装置２０では、ある入力データに落とし戸付き一方向性置換h_1を適用して得られる出力データに、さらに、一方向性逆置換h_1^{-1}を適用すると、もとの入力データが得られる。このことは、落とし戸付き一方向性置換h_2と一方向性逆置換h_2^{-1}との関係においても、同様である。すなわち、一方向性逆置換h_2^{-1}は、落とし戸付き一方向性置換h_2の逆置換である。これにより、暗号鍵生成装置２０では、ある入力データに落とし戸付き一方向性置換h_2を適用して得られる出力データに、さらに、一方向性逆置換h_2^{-1}を適用すると、もとの入力データが得られる。

【００５３】

なお、暗号鍵生成装置２０は、落とし戸付き一方向性置換h_1と可換であるが同一でない落とし戸付き一方向性置換h_2を用いる。これにより、落とし戸付き一方向性置換h_1およびh_2を用いて生成されるスクランブル鍵が、全て同一の値を取ることを防止できる。また、一般に、落とし戸付き一方向性置換h_1と一方向性逆置換h_1^{-1}も、可換である。しかし、暗号鍵生成装置２０は、落とし戸付き一方向性置換h_2として一方向性逆置換h_1^{-1}を用いることはない。すなわち、暗号鍵生成装置２０は、一方向性逆置換h_1^{-1}とは異なる落とし戸付き一方向性置換h_2を用いる。これによっても、落とし戸付き一方向性置換h_1およびh_2を用いて生成されるスクランブル鍵が、全て同一の値を取ることを防止できる。

【００５４】

暗号鍵生成装置２０におけるスクランブル鍵および時限鍵の生成の詳細について、以下に説明する。暗号鍵生成装置２０におけるスクランブル鍵および時限鍵の生成は、暗号鍵生成装置２０が、初期鍵データベース２２から、所定の初期暗号鍵を読み出すことに始まる。ここで、初期鍵データベース２２は、複数の異なる初期暗号鍵を格納している。この初期暗号鍵は、１０００ビットのサイズを有する。スクランブル鍵生成部２６は、初期鍵データベース２２にアクセスし、初期鍵データベース２２から一つの初期暗号鍵を無作為に読み出す。

【００５５】

同時に、暗号鍵生成装置２０において、置換関数データベース２４は、上述した落とし戸付き一方向性置換h_1およびh_2、および一方向性逆置換h_1^{-1}およびh_2^{-1}を定義するデータを格納している。そこで、スクランブル鍵生成部２６は、置換関数データベース２４にアクセスし、一方向性逆置換h_1^{-1}の定義データ、および落とし戸付き一方向性置換h_2の定義データを読み出す。すなわち、スクランブル鍵生成部２６は、一方向性逆置換h_1^{-1}を定義するデータに基づき、一方向性逆置換h_1^{-1}の置換演算を行う。また、スクランブル鍵生成部２６は、落とし戸付き一方向性置換h_2を定義するデータに基づき、落とし戸付き一方向性置換h_2の置換演算を行う。

【００５６】

スクランブル鍵生成部２６は、読み出した初期暗号鍵に、少なくとも１回の一方向性逆

置換h_1^{-1}と、少なくとも１回の落とし戸付き一方向性置換h_2とを、それぞれ適用する。これにより、スクランブル鍵生成部２６は、配信データの暗号化に用いられる複数の互いに異なるスクランブル鍵を生成する。例を挙げると、たとえば、スクランブル鍵生成部２６は、初期暗号鍵に、一方向性逆置換h_1^{-1}を１回、かつ、落とし戸付き一方向性置換h_2を１回、それぞれ適用する。これにより、スクランブル鍵生成部２６は、第１スクランブル鍵を生成する。次に、スクランブル鍵生成部２６は、初期暗号鍵に、一方向性逆置換h_1^{-1}を２回、かつ、落とし戸付き一方向性置換h_2を２回、それぞれ適用する。これにより、スクランブル鍵生成部２６は、第２スクランブル鍵を生成する。

【００５７】

このように、スクランブル鍵生成部２６は、初期暗号鍵に、一方向性逆置換h_1^{-1}をｎ回、かつ、落とし戸付き一方向性置換h_2をｎ回、それぞれ適用する（ｎは１以上の整数）。これにより、スクランブル鍵生成部２６は、ｎ個の互いに異なる複数のスクランブル鍵を生成する。スクランブル鍵生成部２６は、生成したスクランブル鍵を、配信データ暗号化部１２に出力する。また、スクランブル鍵生成部２６は、生成した複数のスクランブル鍵のうち、いずれか１つを時限鍵生成部２８に出力する。このスクランブル鍵は、時限鍵生成部２８が時限鍵を生成する際の、元になるデータである。

【００５８】

時限鍵生成部２８には、スクランブル鍵生成部２６によって生成された複数のスクランブル鍵のいずれか１つが入力される。また、時限鍵生成部２８は、置換関数データベース２４にアクセスし、一方向性逆置換h_1^{-1}を定義するデータを読み出す。すなわち、時限鍵生成部２８は、当該読み出した定義データに基づき、一方向性逆置換h_1^{-1}の置換演算を行う。

【００５９】

ここで、時限鍵生成部２８は、入力されたスクランブル鍵に、少なくとも１回の一方向性逆置換h_1^{-1}を適用する。たとえば、時限鍵生成部２８は、スクランブル鍵に、１回の一方向性逆置換h_1^{-1}を適用することによって、第１の時限鍵を生成する。また、時限鍵生成部２８は、スクランブル鍵に、３回の一方向性逆置換h_1^{-1}を適用することによって、第３の時限鍵を生成する。すなわち、時限鍵生成部２８は、スクランブル鍵に適用する一方向性逆置換h_1^{-1}の回数を変更することによって、異なる範囲のスクランブル鍵系列を再生成可能な時限鍵を生成する。なお、時限鍵生成部２８は、生成した時限鍵を、時限鍵配信部１６に出力する。

【００６０】

暗号鍵生成装置２０によって生成されるスクランブル鍵および時限鍵を用いて、暗号化データ配信システム１において、時間限定型の配信データ配信を行う際の動作の一例を、図１を参照して説明する。図１に示すように、暗号化データ配信装置１０は、配信データ暗号化部１２、暗号化データ配信部１４、時限鍵配信部１６を備えている。

【００６１】

暗号化データ配信装置１０において、配信データ暗号化部１２に、配信される配信データが入力される。また、配信データ暗号化部１２に、暗号鍵生成装置２０によって生成されたスクランブル鍵も、入力される。配信データ暗号化部１２は、入力されたスクランブル鍵を用いて、入力された配信データを、暗号化する。これにより、配信データ暗号化部１２は、暗号化データを生成する。配信データ暗号化部１２は、生成した暗号化データを、暗号化データ配信部１４に出力する。暗号化データ配信部１４は、入力された暗号化データを、通信ネットワークを通じて暗号化データ受信装置３０に配信する。

【００６２】

一方、暗号化データ配信装置１０において、時限鍵配信部１６には、暗号鍵生成装置２０によって生成された時限鍵が入力される。暗号化データ配信装置１０は、入力された時限鍵を、通信ネットワークを通じて、暗号化データ受信装置３０に配信する。

【００６３】

暗号化データ受信装置３０において、時限鍵受信部３２は、配信された時限鍵を受信す

る。時限鍵入力手段は、受信した時限鍵をスクランブル鍵再生成部３３に出力する。スクランブル鍵再生成部３３は、置換関数データベース３１にアクセスして、落とし戸付き一方向性置換h_1の定義データ、および落とし戸付き一方向性置換h_2の定義データを読み出す。すなわち、スクランブル鍵生成部２６は、落とし戸付き一方向性置換h_1を定義するデータに基づき、時限鍵に落とし戸付き一方向性置換h_1を適用する。また、スクランブル鍵生成部２６は、落とし戸付き一方向性置換h_2を定義するデータに基づき、時限鍵に落とし戸付き一方向性置換h_2の適用する。

【００６４】

ここで、スクランブル鍵再生成部３３は、入力された時限鍵に、落とし戸付き一方向性置換h_1および落とし戸付き一方向性置換h_2の少なくともいずれかを適用する。スクランブル鍵再生成部３３は、暗号鍵生成装置２０によって生成された複数のスクランブル鍵の一部を再生成する。スクランブル鍵再生成部３３は、再生成したスクランブル鍵を、配信データ復号化部３５に出力する。

【００６５】

暗号化データ受信部３４は、暗号化データ配信装置１０によって配信された暗号化データを受信する。暗号化データ受信部３４は、受信した暗号化データを、配信データ復号化部３５に出力する。配信データ復号化部３５は、入力されたスクランブル鍵を用いて、暗号化データを復号化する。これにより、配信データ復号化部３５は、配信データを復元する。配信データ復号化部３５は、復元した配信データを、所定の出力先に出力する。これにより、配信データに基づくたとえば動画の再生や、放送の視聴など、暗号化データ配信システム１において提供するコンテンツのユーザ側における限定的利用が可能となる。

【００６６】

スクランブル鍵再生成部３３は、時限鍵に基づき、暗号鍵生成装置２０によって生成されるスクランブル鍵のうち、一部のみを生成できる。換言すると、スクランブル鍵再生成部３３は、時限鍵に落とし戸付き一方向性置換h_1や落とし戸付き一方向性置換h_2をどれだけ適用したところで、スクランブル鍵のうちのあらかじめ定められた一部しか再生成できない。したがって、スクランブル鍵再生成部３３から再生成されたスクランブル鍵の提供を受ける暗号化データ受信装置３０は、スクランブル鍵によって暗号化された配信データの一部のみ、復号化できる。これにより、配信される暗号化データの一部のみが、ユーザ側で利用可能となる。

【００６７】

暗号鍵生成装置２０によって生成されるスクランブル鍵のうち、スクランブル鍵再生成部３３が、時限鍵を用いて一部だけを再生成できる原理について、図３を参照して説明する。図３は、暗号鍵生成装置２０におけるスクランブル鍵および時限鍵の算出原理、および、スクランブル鍵再生成部３３におけるスクランブル鍵の再生成原理を示す説明図である。

【００６８】

図３に示す例において、スクランブル鍵k_1は初期暗号鍵であり、かつ、スクランブル鍵でもある。この図に示すように、スクランブル鍵生成部２６は、スクランブル鍵k_1に、１回の一方向性逆置換h_1^{-1}と、１回の落とし戸付き一方向性置換h_2とを適用する。これにより、スクランブル鍵生成部２６は、スクランブル鍵k_2を生成する。続けて、スクランブル鍵生成部２６は、スクランブル鍵k_2に、１回の一方向性逆置換h_1^{-1}と、１回の落とし戸付き一方向性置換h_2とを適用する。これにより、スクランブル鍵生成部２６は、スクランブル鍵k_3を生成する。

【００６９】

すなわち、スクランブル鍵生成部２６は、１回の一方向性逆置換h_1^{-1}と１回の落とし戸付き一方向性置換h_2とを、生成したスクランブル鍵に再帰的に適用する。これにより、スクランブル鍵生成部２６は、互いに異なる複数のスクランブル鍵を、配信データの暗号化に用いられるスクランブル鍵系列k_1～k_nとして、生成する。

【００７０】

ここで、時限鍵生成部２８が、たとえば、スクランブル鍵系列k_1～k_nのうち、スクランブル鍵k_1～スクランブル鍵k_4までのスクランブル鍵のみを再生成できる時限鍵を生成することを求められたとする。このとき、時限鍵生成部２８は、スクランブル鍵k_1に３回、一方向性逆置換h_1^{-1}を適用することによって、時限鍵$g_{1,4}$を生成する。

【００７１】

これにより、暗号化データ受信装置３０では、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$を用いて、スクランブル鍵k_1に始まるスクランブル鍵系列k_1～k_nの一部分を、再生成する。このとき、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$を用いた場合、最大でも、スクランブル鍵k_1、スクランブル鍵k_2、スクランブル鍵k_3、およびスクランブル鍵k_4の、４つのスクランブル鍵のみを、再生成できる。すなわち、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$に、３回の落とし戸付き一方向性置換h_1を適用することによって、スクランブル鍵k_1を生成する。また、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$に、２回の落とし戸付き一方向性置換h_1と、１回の落とし戸付き一方向性置換h_2とを適用することによって、スクランブル鍵k_2を生成する。また、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$に、１回の落とし戸付き一方向性置換h_1と、２回の落とし戸付き一方向性置換h_2とを適用することによって、スクランブル鍵k_3を生成する。また、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$に、３の落とし戸付き一方向性置換h_2を適用することによって、スクランブル鍵k_3を生成する。

【００７２】

ここで、スクランブル鍵再生成部３３が、時限鍵$g_{1,4}$からスクランブル鍵k_5を再生成するためには、時限鍵$g_{1,4}$に、１回の一方向性逆置換h_1^{-1}を適用する必要がある。しかし、スクランブル鍵再生成部３３は、一方向性逆置換h_1^{-1}を用いることができない。なぜなら、上述したように、一方向性逆置換h_1^{-1}は、一般に公開されていないからである。すなわち、置換関数データベース３１には、一方向性逆置換h_1^{-1}を定義するデータは、格納されていない。また、スクランブル鍵再生成部３３が、公開されている落とし戸付き一方向性置換h_1およびh_2に基づき、一方向性逆置換h_1^{-1}を導出することは、スクランブル鍵再生成部３３に落とし戸情報が入力されない限り、極めて困難である。したがって、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$から、スクランブル鍵k_5を再生成できない。同様に、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$を用いた場合、スクランブル鍵k_5以降の全てのスクランブル鍵を再生成することができない。なぜなら、時限鍵$g_{1,4}$から、スクランブル鍵k_5以降のいずれかのスクランブル鍵を再生成するためには、少なくとも１回の一方向性逆置換h_1^{-1}を、時限鍵$g_{1,4}$に適用する必要があるからである。

【００７３】

また、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$を用いて、スクランブル鍵k_1以前のスクランブル鍵を再生成することもできない。なぜなら、スクランブル鍵k_1以前のスクランブル鍵、たとえば図示しないスクランブル鍵k_0やスクランブル鍵k_{-1}を再生成するためには、時限鍵$g_{1,4}$に、少なくとも１回の一方向性逆置換h_2^{-1}を適用する必要があるからである。一方向性逆置換h_1^{-1}と同様に、一方向性逆置換h_2^{-1}も、落とし戸付き一方向性置換h_2の落とし戸情報が一般に公開されていない以上、落とし戸付き一方向性置換h_2から導出することは極めて困難である。したがって、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$を用いて場合、スクランブル鍵k_1以前の全てのスクランブル鍵を再生成することができない。

【００７４】

なお、上述したように、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$から、スクランブル鍵k_4を再生成することは可能である。しかし、このスクランブル鍵k_4を用いたとしても、スクランブル鍵再生成部３３は、スクランブル鍵k_5以降のスクランブル鍵を再生成することができない。なぜなら、スクランブル鍵k_4からスクランブル鍵k_5以降のスクランブル鍵を生成するためには、スクランブル鍵k_4に、必ず、少なくとも１回の一方向性逆置換h_2^{-1}を適用する必要があるからである。すなわち、スクランブル鍵再

生成部３３は、再生成した、限定された一部のスクランブル鍵を用いたとしても、その範囲を超える他のスクランブル鍵を生成することはできない。具体的には、スクランブル鍵再生成部３３は、時限鍵$g_{1,4}$から再生成できるどのような暗号鍵に基づいても、スクランブル鍵系列k_1～k_nの中では、スクランブル鍵k_1～スクランブル鍵k_4までしか再生成できない。

【００７５】

このように、スクランブル鍵再生成部３３は、時限鍵として時限鍵$g_{1,4}$を用いた場合、スクランブル鍵系列k_1～k_nのうち、スクランブル鍵k_1～スクランブル鍵k_4までしか、再生成できない。すなわち、スクランブル鍵再生成部３３は、生成されるスクランブル鍵のうち、一部分を再生成できるのみである。なお、スクランブル鍵再生成部３３が再生成できるスクランブル鍵の範囲は、用いる時限鍵に依存する。すなわち、異なる時限鍵を用いた場合、スクランブル鍵再生成部３３は、スクランブル鍵系列k_1～k_nのうち、異なる範囲を再生成できる。

【００７６】

たとえば、図３に示す例では、スクランブル鍵再生成部３３は、時限鍵として時限鍵$g_{2,6}$を用いる場合、スクランブル鍵k_2～スクランブル鍵k_6を再生成できる。なお、この時限鍵$g_{2,6}$は、暗号鍵生成装置２０において、時限鍵生成部２８が、スクランブル鍵k_2に一方向性逆置換h_1^{-1}を４回適用することによって、生成される。スクランブル鍵再生成部３３は、時限鍵$g_{2,6}$に、落とし戸付き一方向性置換h_1と落とし戸付き一方向性置換h_2とを適宜適用して、スクランブル鍵を再生成する。ここで、図３に示すように、時限鍵$g_{2,6}$からは、スクランブル鍵k_2～スクランブル鍵k_6までは、いずれも、落とし戸付き一方向性置換h_1および落とし戸付き一方向性置換h_2の適用で再生成できる。しかし、上述したように、時限鍵$g_{2,6}$に基づき、スクランブル鍵k_1以前のスクランブル鍵を再生成する場合、必ず、最低１回の一方向性逆置換h_2^{-1}を適用する必要が生ずる。また、時限鍵$g_{2,6}$に基づき、スクランブル鍵k_7以降のスクランブル鍵を再生成する場合、必ず、最低１回の一方向性逆置換h_1^{-1}を適用する必要が生ずる。したがって、スクランブル鍵再生成部３３が時限鍵$g_{2,6}$に基づいて再生成できるスクランブル鍵は、スクランブル鍵k_2～スクランブル鍵k_6に限定される。

【００７７】

なお、他の例を説明すると、図３に示すように、スクランブル鍵再生成部３３は、時限鍵として時限鍵$g_{5,7}$を用いる場合、スクランブル鍵k_5～スクランブル鍵k_7のみを再生成できる。なお、この時限鍵$g_{5,7}$は、暗号鍵生成装置２０において、時限鍵生成部２８が、スクランブル鍵k_5に一方向性逆置換h_1^{-1}を２回適用することによって、生成される。スクランブル鍵再生成部３３は、時限鍵$g_{5,7}$に、落とし戸付き一方向性置換h_1と落とし戸付き一方向性置換h_2とを適宜適用して、スクランブル鍵を再生成する。ここで、図３に示すように、時限鍵$g_{5,7}$からは、スクランブル鍵k_5～スクランブル鍵k_7までは、いずれも、落とし戸付き一方向性置換h_1および落とし戸付き一方向性置換h_2の適用のみで再生成できる。しかし、上述したように、時限鍵$g_{5,7}$に基づき、スクランブル鍵k_4以前のスクランブル鍵を再生成する場合、必ず、最低１回の一方向性逆置換h_2^{-1}を適用する必要が生ずる。また、時限鍵$g_{5,7}$に基づき、スクランブル鍵k_8以降のスクランブル鍵を再生成する場合、必ず、最低１回の一方向性逆置換h_1^{-1}を適用する必要が生ずる。したがって、スクランブル鍵再生成部３３が時限鍵$g_{5,7}$に基づいて再生成できるスクランブル鍵は、スクランブル鍵k_5～スクランブル鍵k_7に限定される。

【００７８】

以上のように、暗号鍵生成装置２０において、スクランブル鍵生成部２６は、スクランブル鍵を生成する際、必ず、最低１回の一方向性逆置換h_1^{-1}と、最低１回の落とし戸付き一方向性置換h_2とを適用する。したがって、スクランブル鍵生成部２６によって生成されるスクランブル鍵からは、スクランブル鍵に一方向性逆置換h_1^{-1}や一方向性逆置換h_2^{-1}を適用しない限り、他のスクランブル鍵を生成することはできない。すなわ

ち、スクランブル鍵生成部２６によって生成されるスクランブル鍵は、ユーザが利用する暗号化データ受信装置３０において、他のスクランブル鍵に相互変換されることがない。

【００７９】

一方、暗号鍵生成装置２０において、時限鍵生成部２８は、時限鍵を生成する際、初期暗号鍵に、最低１回の一方向性逆置換h_1^{-1}を適用する。したがって、スクランブル鍵再生成部３３は、時限鍵に、落とし戸付き一方向性置換h_1や落とし戸付き一方向性置換h_2を適宜適用することによって、複数のスクランブル鍵のうち一部のみを再生成できる。このように、暗号鍵生成装置２０は、配信データの暗号化および復号化に用いられる複数のスクランブル鍵、および、スクランブル鍵の一部のみを再生成可能な時限鍵を効率的かつ柔軟に生成できる。

【００８０】

そのため、暗号鍵生成装置２０によって生成されるスクランブル鍵および時限鍵を用いて、暗号化データをストリーミング配信すれば、配信された配信データを利用できる期間を、あらかじめ限定できる。その一例を、以下に説明する。

【００８１】

まず、暗号化データ配信装置１０は、クロック手段によって生成される所定のクロック信号に基づき、暗号化データをストリーミング配信する。すなわち、たとえば、暗号鍵生成装置２０におけるスクランブル鍵生成部２６が、所定のクロック信号に同期させて、所定間隔（たとえば１分）で、異なるスクランブル鍵を次々と生成する。これにより、スクランブル鍵生成部２６は、短期間に大量のスクランブル鍵を、次々と更新していく。一方、配信データ暗号化部１２は、所定間隔で異なるスクランブル鍵に更新されていく複数のスクランブル鍵を用いて、複数の配信データを、それぞれ暗号化する。これにより、暗号化データ配信部１４は、異なる時間に、異なるスクランブル鍵によって暗号化された配信データを、暗号化データ受信装置３０に配信する。

【００８２】

一方、スクランブル鍵再生成部３３は、時限鍵に基づき、一部のスクランブル鍵、すなわち、所定の制限期間内に配信された暗号化データを復号化するスクランブル鍵のみを、生成する。そのため、暗号化データ受信装置３０は、スクランブル鍵再生成部３３によって復号化されたスクランブル鍵を用いて、所定期間内に配信された暗号化データのみを、復号化できる。このように、暗号鍵生成装置２０を利用すれば、時間限定型の情報提供システムを提供できる。

【００８３】

以上に説明したように、本発明に係る暗号鍵生成装置２０は、一般に公開する、可換な第１および落とし戸付き一方向性置換h_2と、落とし戸付き一方向性置換h_1の逆置換であり、かつ、一般に非公開にする一方向性逆置換h_1^{-1}と、落とし戸付き一方向性置換h_2の逆置換であり、かつ、一般に非公開にする一方向性逆置換h_2^{-1}とを用いて暗号鍵を生成する暗号鍵生成方法であって、所定の初期暗号鍵に、少なくとも１回の一方向性逆置換h_1^{-1}と、少なくとも１回の落とし戸付き一方向性置換h_2とをそれぞれ適用することによって、配信データの暗号化に用いられる複数の互いに異なるスクランブル鍵を生成する個別暗号鍵生成工程と、生成された複数のスクランブル鍵のいずれかに、一方向性逆置換h_1^{-1}および一方向性逆置換h_2^{-1}の少なくとも一方を、少なくとも１回適用することによって、時限鍵を生成するマスタ暗号鍵生成工程とを含んでいる暗号鍵生成方法を実行する装置である。

【００８４】

なお、本発明は上述した実施形態に限定されるものではなく、請求項に示した範囲で種々の変更が可能である。すなわち、請求項に示した範囲で適宜変更した技術的手段を組み合わせて得られる実施形態についても、本発明の技術的範囲に含まれる。

【００８５】

たとえば、暗号化データ配信装置１０は、時限鍵を、暗号化データ受信装置３０に固有に割り当てられた端末暗号鍵によって暗号化する時限鍵暗号化手段を備えていてもよい。

この構成によると、暗号化データ配信装置１０は、特定の端末においてのみ元の形式に復元可能な時限鍵を、通信ネットワークによって暗号化データ受信装置３０に配信できる。したがって、不正な第３者によって用いられる暗号化データ受信装置３０が、入力された時限鍵を用いてスクランブル鍵を再生成することを防止できる。

【００８６】

なお、暗号化データ配信装置１０は、必ずしも、時限鍵配信部１６を備えている必要はない。たとえば、暗号化データ配信システム１では、暗号化データ配信装置１０において、暗号鍵生成装置２０によって生成された時限鍵を何らかの記録媒体に格納して、暗号化データ受信装置３０を用いるユーザに販売してもよい。この場合、ユーザは、入手した記録媒体から、時限鍵を暗号化データ受信装置３０に入力する。すなわち、暗号化データ受信装置３０は、時限鍵の入力を受け付ける時限鍵入力手段を備え、時限鍵の入力を受け付ける。暗号化データ受信装置３０は、入力された時限鍵を用いて、スクランブル鍵を再生成する。

【００８７】

暗号鍵生成装置２０が用いる落とし戸付き一方向性置換h_1およびh_2は、いずれも、ＲＳＡ関数であることが好ましい。すなわち、暗号鍵生成装置２０は、落とし戸付き一方向性置換h_1としてx^{e_1}（ｍｏｄ　ｎ）を用い、かつ、落とし戸付き一方向性置換h_2としてx^{e_2}（ｍｏｄ　ｎ）を用いることが好ましい。ここで、ｘは、適用される入力データである。ｐおよびｑは、互いに異なる素数である。ｎは、ｐ×ｑである。b_0、b_1、b_2は、それぞれ、ｐ－１とｑ－１との最小公約数と互いに素な正の整数である。e_1は、$b_0 \times b_1$である。e_2は、$b_0 \times b_2$である。ｎ、e_1、およびe_2を、一般に公開する。すでに知られているように、一般に公開されたｎ、e_1、およびe_2に基づいても、落とし戸情報を知らない限り、x^{e_1}（ｍｏｄ　ｎ）の逆関数や、x^{e_2}（ｍｏｄ　ｎ）の逆関数を求めることは極めて困難である。

【００８８】

このように、暗号鍵生成装置２０を、広く流通しているＲＳＡ関数を用いた構成とすることができる。これにより、実用的な暗号強度を有するスクランブル鍵および時限鍵を生成できる。

【００８９】

また、暗号鍵生成装置２０が用いる落とし戸付き一方向性置換h_1およびh_2は、互いに、直交一方向性を満たしていることが好ましい。これにより、一般に公開する落とし戸付き一方向性置換h_1およびh_2から、落とし戸情報を知らずに一方向性逆置換h_1^{-1}およびh_2^{-1}を導出できる可能性が、より低くなる。したがって、生成されるスクランブル鍵および時限鍵の秘匿性を、より高めることができる。

【００９０】

また、スクランブル鍵生成部２６は、生成したスクランブル鍵に、少なくとも１回の一方向性逆置換h_1^{-1}と、少なくとも１回の落とし戸付き一方向性置換h_2とを適用してもよい。これにより、スクランブル鍵生成部２６は、異なる新たなスクランブル鍵を生成できる。このとき、スクランブル鍵生成部２６は、生成したスクランブル鍵を新たな入力データとして、新たなスクランブル鍵を再帰的に生成する。したがって、暗号鍵生成装置２０は、一連のスクランブル鍵系列$k_1 \sim k_n$を、効率的に生成できる。

【００９１】

また、暗号化データ受信装置３０に備えられるスクランブル鍵再生成部３３は、単独構成の装置であってよい。すなわち、本発明に係るスクランブル鍵再生成装置（個別鍵再生成装置）は、入力された時限鍵に落とし戸付き一方向性置換h_1および落とし戸付き一方向性置換h_2の少なくともいずれかを適用することによって、暗号鍵生成装置２０によって生成された複数のスクランブル鍵のうち一部のスクランブル鍵を再生成する装置であればよい。

【００９２】

また、初期暗号鍵のサイズは、１０００ビットに限らず、任意のサイズ（好ましくは１

０００ビット以上）であってよい。

【００９３】

また、スクランブル鍵生成部２６は、所定のクロック信号に同期させて、１分に限らず、任意の所定間隔（たとえば、１ミリ秒、１００ミリ秒、１分、１０分等）で、異なるスクランブル鍵を次々と生成してもよい。

【００９４】

また、時限鍵生成部２８は、入力されたスクランブル鍵のうちいずれか１つに、一方向性逆置換h_1^{-1}およびh_2^{-1}のうち、少なくともいずれかを、少なくとも１回適用することによって、時限鍵を生成するものであればよい。すなわち、時限鍵生成部２８は、スクランブル鍵に、１回の一方向性逆置換h_1^{-1}と、１回の一方向性逆置換h_2^{-1}とを適用することによって、時限鍵を生成してもよい。また、時限鍵生成部２８は、スクランブル鍵に、３回の一方向性逆置換h_2^{-1}とを適用することによって、時限鍵を生成してもよい。なお、このとき時限鍵生成部２８が用いる一方向性逆置換h_2^{-1}を定義するデータも、一方向性逆置換h_1^{-1}を定義するデータと同様に、置換関数データベース２４に格納されている。さらに、時限鍵生成部２８は、適用する一方向性逆置換h_1^{-1}およびh_2^{-1}の回数を増やすほど、カバーする範囲がより広い時限鍵を生成できる。

【００９５】

図３に示す時限鍵$g_{2,6}$の生成を例に挙げると、時限鍵生成部２８は、図３に示すスクランブル鍵k_6に４回の一方向性逆置換h_2^{-1}を適用することによっても、時限鍵$g_{2,6}$を生成できる。さらに、図３に示すスクランブル鍵k_5に１回の一方向性逆置換h_1^{-1}と、３回の一方向性逆置換h_2^{-1}を適用することによっても、時限鍵$g_{2,6}$を生成できる。さらに、図３に示すスクランブル鍵k_4に２回の一方向性逆置換h_1^{-1}と、２回の一方向性逆置換h_2^{-1}を適用することによっても、時限鍵$g_{2,6}$を生成できる。

【００９６】

また、上述した初期暗号鍵は、スクランブル鍵としても機能する。ここで、時限鍵生成部２８には、初期暗号鍵が入力されてもよい。このとき、時限鍵生成部２８は、入力された初期暗号鍵に、一方向性逆置換h_1^{-1}およびh_2^{-1}のうち、少なくともいずれかを、少なくとも１回適用することによって、時限鍵を生成する。これによっても、時限鍵生成部２８は、スクランブル鍵生成部２６によって生成される複数のスクランブル鍵のうち一部のみを再生成できる時限鍵を作成できる。

【００９７】

以上に説明したように、暗号鍵生成装置２０では、ユーザが利用する端末としての暗号化データ受信装置３０に、第３者に公開できない、特定の情報や手順をあらかじめ備えておく必要がない。したがって、暗号化データ受信装置３０は、特殊な高タンパ性を有するハードウェアを利用することなく、時間限定型の情報提供サービスに利用可能なスクランブル鍵を再生成できる。すなわち、暗号化データ受信装置３０を、特殊なハードウェアを組み込む端末装置に比べて、より安価に実現できる。

【００９８】

また、暗号鍵生成装置２０は、柔軟な期限設定を可能な時限鍵を生成できる。暗号鍵生成装置２０では、一方向性逆置換h_1^{-1}を用いて、時限鍵を生成する。これにより、生成される時限鍵のサイズは、カバーするスクランブル鍵の数にかかわらず、一定となる。したがって、大量のスクランブル鍵を再生成できる時限鍵を生成したとしても、時限鍵のサイズに変化はない。これにより、時限鍵などの暗号化情報を、非常にコンパクトにやり取りできる。

【００９９】

暗号化データ配信システム１では、暗号化データ受信装置３０に提供された時限鍵は、所定の規定期間の開始後、自立的に有効となる一方で、当該規定期間の終了後、自立的に無効となる。このため、暗号化データ配信装置１０において、暗号化データ受信装置３０に配信する時限鍵を管理する必要がない。これにより、暗号化データ配信装置１０を用い

てコンテンツを提供する管理者の手間を軽減できる。

【０１００】

また、暗号鍵生成装置２０では、時限鍵に対して、所定回数の落とし戸付き一方向性置換h_1およびh_2の一方を適用することによって、スクランブル鍵のいずれかを再生成できる。また、スクランブル鍵から、他のスクランブル鍵を生成するためには、一方向性逆置換h_1^{-1}およびh_2^{-1}の少なくともいずれか一方を適用する必要がある。これが極めて困難であることから、暗号鍵生成装置２０によって生成される時限鍵は、リバースエンジニアリング等による不正解読に対する耐性が極めて高いすなわち、暗号鍵生成装置２０を備えることによって、暗号強度が非常に高い暗号化データ配信システム１を提供できる。

【０１０１】

なお、上述した各部材（各手段）は、いずれも機能ブロックである。したがって、これらの部材は、ＣＰＵなどの演算手段が、図示しない記憶部に格納された暗号鍵生成プログラムを実行し、図示しない入出力回路などの周辺回路を制御することによって、実現される。

【０１０２】

したがって、本発明の目的は、上述した機能を実現するソフトウェアである暗号鍵生成プログラムのプログラムコード（実行形式プログラム、中間コードプログラム、ソースプログラム）をコンピュータによって読み取り可能に記録している記録媒体を、暗号鍵生成装置に供給し、暗号鍵生成装置に備えられるコンピュータ（またはＣＰＵやＭＰＵ、ＤＳＰ）が、記録媒体に記録されているプログラムコードを読み出し実行することによって、達成可能である。

【０１０３】

この場合、記録媒体から読み出されたプログラムコード自体が上述した機能を実現することになり、そのプログラムコードを記録している記録媒体は本発明を構成することになる。

【０１０４】

一方で、上述した各部材は、上述したソフトウェアと同様の処理を行うハードウェアとして実現してもよい。この場合、本発明の目的は、ハードウェアとしての暗号鍵生成装置によって達成されることになる。

【０１０５】

ここで、プログラムコードを読み出し実行する演算手段は、単体の構成であればよい。または、暗号鍵生成装置内部のバスや各種の通信路を介して接続されている複数の演算手段が、プログラムコードを協同して実行する構成であってもよい。

【０１０６】

ここで、演算手段によって直接的に実行可能なプログラムコードは、このプログラムコードを格納しているコンピュータ読み取り可能な記録媒体を通じて、暗号鍵生成装置に配布すればよい。また、プログラムコードを、後述する解凍などの処理によってプログラムコードを生成可能なデータとして、当該データを格納しているコンピュータ読み取り可能な記録媒体に通じて、暗号鍵生成装置に配布してもよい。あるいは、これらのプログラムコードまたはデータを、有線または無線の通信路を介してデータを伝送する通信ネットワークを通じて、暗号鍵生成装置に配布または送信してもよい。いずれの手段によって配布または送信されても、プログラムコードは、暗号鍵生成装置に備えられる演算手段によって実行される。

【０１０７】

このとき、特定のものに限定されない各種の通信ネットワークを通じて、プログラムコードまたはデータを伝送できる。このような通信ネットワークの具体例を挙げると、インターネット、イントラネット、エキストラネット、ＬＡＮ、ＩＳＤＮ、ＶＡＮ、ＣＡＴＶ通信網、仮想専用網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）、電話回線網、移動体通信網、衛星通信網等がある。また、通信ネットワークを構成する伝送媒体（通

信路）も、特に限定されない。具体的には、ＩＥＥＥ１３９４規格による回線、ＵＳＢ回線、電力線、ケーブルＴＶ回線、電話線、およびＡＤＳＬ回線等の有線を、伝送媒体として利用できる。また、ＩｒＤＡやリモコンに用いられている赤外線を利用した無線、Ｂｌｕｅｔｏｏｔｈ規格またはＩＥＥＥ８０２．１１無線規格に規定されている無線、ＨＤＲ、携帯電話網、衛星回線、地上波デジタル網等を利用した無線も、伝送媒体として利用できる。

【０１０８】

なお、プログラムコードを暗号鍵生成装置に配布するための記録媒体は、プログラムコードの配布前には、取り外し可能になっていることが好ましい。しかし、プログラムコードを配布した後には、暗号鍵生成装置装置から取り外し可能になっていてもよく、暗号鍵生成装置と一体化されて取り外し不可能になっていてもよい。

【０１０９】

また、記録媒体は、プログラムコードが記録されてさえいれば、書き換え（書き込み）可能であってもよく、不可能であってもよい。また、揮発性であってもよく、非揮発性であってもよい。また、記録媒体へのプログラムコードの記録方法、および記録媒体の形状も、任意のものでよい。

【０１１０】

このような条件を満たす記録媒体を例示すると、磁気テープやカセットテープなどのテープ、フロッピー（登録商標）ディスクやハードディスクなどの磁気ディスク、ＣＤ－ＲＯＭや光磁気ディスク（ＭＯ）、ミニディスク（ＭＤ）、デジタルビデオディスク（ＤＶＤ）などのディスクがある。また、ＩＣカードや光カードのようなカード型メモリ、あるいは、マスクＲＯＭやＥＰＲＯＭ、ＥＥＰＲＯＭまたはフラッシュＲＯＭなどの半導体メモリも該当する。さらに、ＣＰＵなどの演算手段内に形成されているメモリも該当する。

【０１１１】

なお、プログラムコードを記録媒体から読み出して主記憶に格納するためのプログラムは、あらかじめ、暗号鍵生成装置内に、コンピュータによって実行可能に格納されている。また、プログラムコードを通信ネットワークを通じて暗号鍵生成装置に配布する場合、通信ネットワークからプログラムコードをダウンロードするプログラムは、あらかじめ、暗号鍵生成装置内に、コンピュータによって実行可能に格納されている。

【０１１２】

また、プログラムコードは、上述した各処理の全手段を演算手段へ指示するコードであればよい。なお、コンピュータには、プログラムコードによる各処理の一部または全部を所定の手順で呼び出すことによって実行可能な基本プログラム（たとえば、オペレーティングシステムやライブラリなど）がすでに存在している場合がある。この場合、プログラムコードにおける全手順の一部または全部を、この基本プログラムの呼び出しを演算手段へ指示するコードやポインタなどに置き換えたプログラムコードものを、暗号鍵生成プログラムのプログラムコードとしてもよい。

【０１１３】

また、記録媒体には、実メモリにプログラムコードを配置した状態のように、暗号鍵生成プログラムを格納すればよい。具体的には、演算手段が記録媒体にアクセスしてプログラムコードを実行できる形式によって、暗号鍵生成プログラムを記録媒体に格納すればよい。または、実メモリにプログラムコードを配置する前であり、かつ、演算手段が常時アクセス可能なローカルな記録媒体（たとえばハードディスクなど）にインストールした後の格納形式によって、暗号鍵生成プログラムを記録媒体に格納してもよい。あるいは、通信ネットワークや搬送可能な記録媒体などからローカルな記録媒体にインストールする前の格納形式によって、暗号鍵生成プログラムを記録媒体に格納してもよい。

【０１１４】

また、暗号鍵生成プログラムは、コンパイルされた後のオブジェクトコードに限られない。たとえば、暗号鍵生成プログラムは、ソースコードとして記録媒体に格納されていてもよい。あるいは、インタプリトまたはコンパイルの途中において生成される中間コード

として、記録媒体に格納されていてもよい。

【０１１５】

上述したいずれの場合であっても、記録媒体に格納されているプログラムコード（中間コード）は、演算手段が実行可能な形式に変換可能なものであればよい。

【０１１６】

すなわち、プログラムコード（中間コード）は、所定の形式変換プログラムが、圧縮されたプログラムコードを解凍したり、符号化されたプログラムコードを復元したり、ソースコードをインタプリト、コンパイル、リンク、または、実メモリへ配置したりすることによって、あるいはこれらの処理を組み合わせて実行することによって、演算手段が実行可能な形式に変換されるものであればよい。これにより、暗号鍵生成プログラムを記録媒体に格納する際の格納形式にかかわらず、同様の効果を得ることができる。

【０１１７】

なお、本発明は上述した実施形態に限定されるものではなく、請求項に示した範囲で種々の変更が可能である。すなわち、請求項に示した範囲で適宜変更した技術的手段を組み合わせて得られる実施形態についても、本発明の技術的範囲に含まれる。

【産業上の利用可能性】

【０１１８】

本発明は、たとえば、公共のホットスポットサービス等など、ユーザのニーズに応じた、時間限定型のネットワークアクセスサービスに利用できる。さらに、特定の時間帯に視聴可能な番組を、スクランブル放送する形態にも応用できる。たとえば、夜間限定の視聴サービスを割安で提供することに応用できる。また、時限鍵をＩＣカードなどにマスター鍵として格納することによって、特定の施設への入退室を、特定の時間帯においてのみ認めるサービスにも応用できる。また、時間限定型の無線ＬＡＮサービスの提供や、各種メディアの体験版を利用するサービスの提供にも応用できる。また、使用できるソフトウェアやデータベース、あるいは、ログイン可能なサーバに制限をかけるサービスにも応用できる。

【図面の簡単な説明】

【０１１９】

【図１】本発明に係る暗号鍵生成装置の構成を詳細に示すブロック図である。

【図２】本発明に係る暗号化データ配信システムの構成を詳細に示すブロック図である。

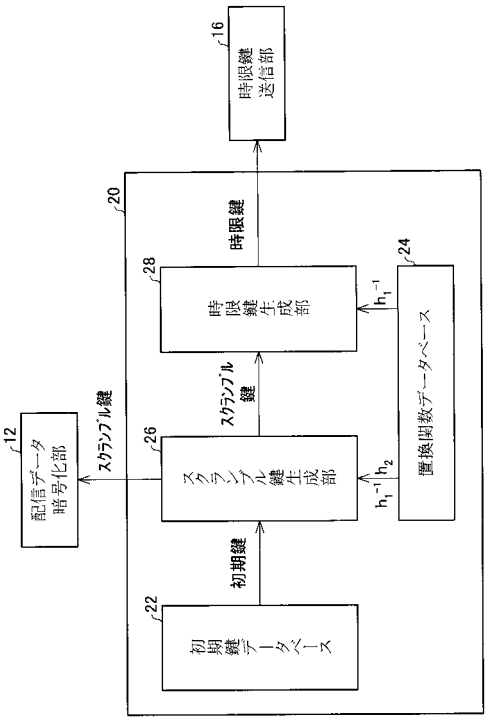
【図３】本発明におけるスクランブル鍵および時限鍵の算出原理を示す説明図である。

【符号の説明】

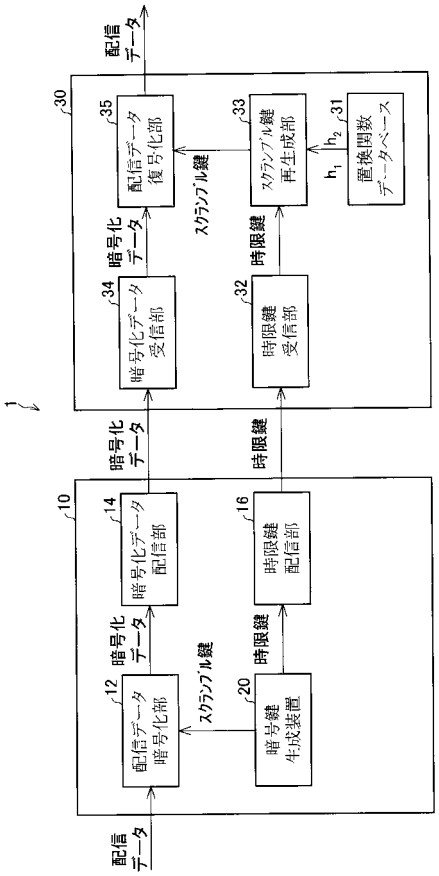
【０１２０】

１　暗号化データ配信システム
１０　暗号化データ配信装置
１２　配信データ暗号化部（暗号化データ生成手段）
１６　時限鍵配信部（マスタ暗号鍵配信手段）
２０　暗号鍵生成装置
２２　初期鍵データベース
２４　置換関数データベース
２６　スクランブル鍵生成部（個別暗号鍵生成手段）
２８　時限鍵生成部（マスタ暗号鍵生成手段）
３０　暗号化データ受信装置
３１　置換関数データベース
３２　時限鍵受信部（暗号化データ受信装置）
３３　スクランブル鍵再生成部（個別暗号鍵再生成手段）
３４　暗号化データ受信部
３５　配信データ復号化部（配信データ復号化手段）

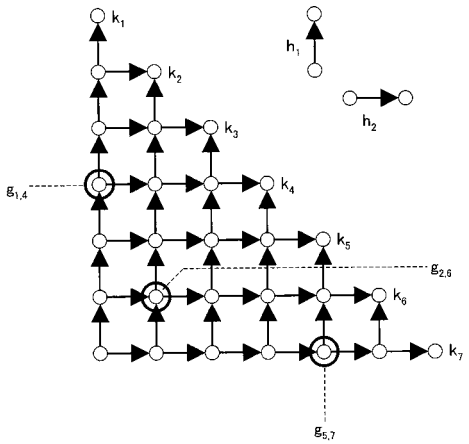
【図１】


16
時限鍵送信部
20
時限鍵
28
時限鍵生成部
24
h_1^{-1}
スクランブル鍵
26
スクランブル鍵生成部
h_1^{-1} h_2
置換関数データベース
12
配信データ暗号化部
スクランブル鍵
初期鍵
22
初期鍵データベース

【図２】


配信データ
30
35
配信データ復号化部
33
スクランブル鍵再生成部
h_1 h_2
31
置換関数データベース
スクランブル鍵
暗号化データ
34
暗号化データ受信部
32
時限鍵受信部
時限鍵
1
暗号化データ
時限鍵
10
14
暗号化データ配信部
16
時限鍵配信部
暗号化データ
12
配信データ暗号化部
スクランブル鍵
時限鍵
20
暗号鍵生成装置
配信データ

【図３】


k_1
k_2
k_3
k_4
k_5
k_6
k_7
h_1
h_2
$g_{1,4}$
$g_{2,6}$
$g_{5,7}$

フロントページの続き

(56)参考文献 特開平１１－２９６０７６（ＪＰ，Ａ）
特開平０７－０７２７９３（ＪＰ，Ａ）
野島良，楫勇一，“落とし戸付き一方向性関数を利用した木構造鍵管理方式”，暗号と情報セキュリティシンポジウム（SCIS2003）講演論文集CD-ROM，日本，２００３年 1月２６日，３Ｂ 鍵配送・管理（１），３Ｂ－４
Ryo NOJIMA, Yuichi KAJI, “Secure, Efficient and Practical Key Management Scheme in the Complete-Subtree Method”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 日本，社団法人電子情報通信学会基礎・境界ソサイエティ，[online]，２００５年 1月 1日，ＶＯＬ．Ｅ８８－Ａ，ＮＯ．１，第３９７号，ｐ．１８９－１９４，[検索日：平成２２年１１月 9日]，インターネット，ＵＲＬ，http://ci.nii.ac.jp/naid/110003213225
楫勇一，野島良，“時間限定サービスを実現するための時系列鍵管理方式”，２００５年暗号と情報セキュリティシンポジウム ＳＣＩＳ２００５ 予稿集付録ＣＤ－ＲＯＭ，日本，２００５年 1月２５日，１Ｄ３ 鍵管理，１Ｄ３－４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ 9／０８