(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4358239号
(P4358239)
(45)発行日　平成21年11月4日(2009.11.4)　(24)登録日　平成21年8月14日(2009.8.14)

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

請求項の数 28　(全 41 頁)

(21)出願番号　特願2007-2658(P2007-2658)
(22)出願日　平成19年1月10日(2007.1.10)
(65)公開番号　特開2008-172433(P2008-172433A)
(43)公開日　平成20年7月24日(2008.7.24)
審査請求日　平成20年3月27日(2008.3.27)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】コンテンツ提供システム、追跡システム、コンテンツ提供方法及び不正ユーザ特定方法

(57)【特許請求の範囲】
【請求項１】
複数のユーザシステムを個別に識別するための複数のユーザ識別情報を複数のユーザセグメントに分割し、前記複数のユーザセグメントに対し異なる複数のセッション鍵s_j（j＝１，２，…、ｎ）をそれぞれ割り当てることにより得られる、各ユーザ識別情報に対応するセッション鍵を示す情報を、当該ユーザ識別情報に対応付けて記憶するユーザ区分情報記憶手段と、
前記複数のユーザセグメントのうちの１つである第１のユーザセグメントに属するユーザ識別情報と、他の１つである第２のユーザセグメントに属するユーザ識別情報とを含む複数のユーザ識別情報のグループに対し、前記複数のセッション鍵のうち、前記第１のユーザセグメントに対応する第１のセッション鍵s_1と、前記第２のユーザセグメントに対応する第２のセッション鍵s_2とのそれぞれを用いてコンテンツを暗号化し、前記第１のセッション鍵に対応する第１の暗号化コンテンツと、前記第２のセッション鍵に対応する第２の暗号化コンテンツを生成するコンテンツ暗号化手段と、
前記第１及び第２のセッション鍵のそれぞれを、前記グループ内の各ユーザシステム固有の復号鍵に対応する公開鍵で暗号化し、複数の暗号化セッション鍵を得るセッション鍵暗号化手段と、
前記グループに対し、
（ａ）前記複数の暗号化セッション鍵と、
（ｂ）前記第１及び第２のセッション鍵に対応する第１のベクトル（L_0，L_1，L_2

，…，L_k）とを含み、

前記第１のベクトルは、前記グループ内の任意のユーザ識別情報ｕに関する第２のベクトル（１，ｕ，u^2，…，u^k）との内積が、$z_j u^v$（ここで、ｋは予め定められた正の整数、z_jは前記複数のユーザセグメントに対応する異なる複数の定数値のうち該ユーザ識別情報ｕの属するユーザセグメントに対応する定数値、ｖは前記グループにグループ識別情報として割り当てられた値に基づく「０」以上ｋ以下の整数のうちのいずれか１つの整数）に等しくなるように設定され、

前記グループに属する各ユーザシステムにおいて、当該ユーザシステム固有の復号鍵を用いて、前記第１及び第２のセッション鍵のうち当該ユーザシステムの属するユーザセグメントに割り当てられたセッション鍵が得られる暗号化セッション鍵を復号可能にするヘッダ情報を生成するヘッダ情報生成手段と、

前記第１及び第２の暗号化コンテンツと、前記ヘッダ情報を送信する送信手段と、

を備えたコンテンツ提供システム。

【請求項２】

前記ヘッダ情報生成手段は、前記第１のベクトルと前記第２のベクトルとの内積

【数１】

$$\sum_{i=0}^{2k'-1} L_i u^i$$

（ここで、ｋ′は不正ユーザ識別情報の数に対し予め定められた最大値であり、ｋ＝２ｋ′－１を満たす）が、$z_j u^{v \bmod 2k'}$に等しくなるように、該第１のベクトルを設定することを特徴とする請求項１記載のコンテンツ提供システム。

【請求項３】

各ユーザシステム固有の前記復号鍵は、

ルートのノードから１つ又は複数のノードを介して複数のリーフに至る木構造に、前記ルート、前記複数のノード及び前記複数のリーフ毎にそれぞれ異なる個別鍵生成多項式を割り当てるとともに、当該木構造上の異なる複数のリーフに、前記グループを含む複数のユーザシステムを個別に識別するための複数のユーザ識別情報の集合を分割することにより得られる複数のサブグループをそれぞれ割り当て、当該複数のサブグループのうち、当該ユーザシステムに対応するユーザ識別情報の属するサブグループに割り当てられた当該木構造上のリーフ及びその祖先ノードのそれぞれに対応する前記個別鍵生成多項式のうちの１つと、前記ルート、前記複数のノード及び前記複数のリーフで共通の共通鍵生成多項式とに、当該ユーザシステムのユーザ識別情報を代入することにより得られた値であることを特徴とする請求項１記載のコンテンツ提供システム。

【請求項４】

前記個別鍵生成多項式と前記共通鍵生成多項式の同じ次数の係数の線形和のうちの少なくとも１つは、前記木構造上の前記ルート、前記複数のノード、及び前記複数のリーフ毎にそれぞれ異なり、それ以外の前記同じ次数の係数の線形和は一定であることを特徴とする請求項３記載のコンテンツ提供システム。

【請求項５】

前記木構造上の前記ルート、前記複数のノード、及び前記複数のリーフのうちの１つ（ｖ）に割り当てる前記個別鍵生成多項式A_v（ｘ）及び前記共有鍵生成多項式Ｂ（ｘ）は、

【数２】

$$A_v(x) = \sum_{i=0}^{k_a} (a_{v,i} - \lambda_v b_i) x^i \bmod q$$

$$B(x) = \sum_{i=0}^{k_b} b_i x^i \bmod q$$

（λ_v：前記ルート、前記複数のノード及び前記複数のリーフ毎に固有の定数値、k_a、k_b：任意の正の整数値、ｑ：予め定められた正の整数値）

であり、且つ前記個別鍵生成多項式A_v（ｘ）の係数$a_{v,i}$（ｉ＝０，１，…，k_a）のうちの少なくとも１つの係数$a_{v,n}$（０≦ｎ≦ｋａの整数）は、前記ルート、前記複数のノード及び前記複数のリーフ毎に固有の定数値であることを特徴とする請求項３記載のコンテンツ提供システム。

【請求項６】

前記コンテンツ暗号化手段は、異なる電子透かし情報が埋め込まれている２つのコンテンツを前記第１及び第２のセッション鍵のそれぞれを用いて暗号化し、前記第１の暗号化コンテンツ及び前記第２の暗号化コンテンツを得ることを特徴とする請求項１記載のコンテンツ提供システム。

【請求項７】

前記コンテンツ暗号化手段は、複数の電子透かし情報のうちの第１の電子透かし情報が埋め込まれている第１のコンテンツを前記第１のセッション鍵を用いて暗号化することにより前記第１の暗号化コンテンツを生成し、前記複数の電子透かし情報のうちの前記第１の電子透かし情報とは異なる第２の電子透かし情報が埋め込まれている第２のコンテンツを前記第２のセッション鍵を用いて暗号化することにより前記第２の暗号化コンテンツを生成することを特徴とする請求項１記載のコンテンツ提供システム。

【請求項８】

検査対象のユーザシステムを検査し、複数のユーザシステムを個別に識別するための複数のユーザ識別情報のなかから不正ユーザ識別情報を特定するための追跡システムであって、

第１のセッション鍵s_1と第２のセッション鍵s_2とを用いて、異なる電子透かし情報が埋め込まれている第１及び第２のコンテンツをそれぞれ暗号化し、前記第１のセッション鍵で復号可能な第１の暗号化コンテンツと前記第２のセッション鍵で復号可能な第２の暗号化コンテンツを得るコンテンツ暗号化手段と、

複数のユーザ識別情報を含むグループを、前記第１のセッション鍵を割り当てる第１のユーザセグメントと、前記第２のセッション鍵を割り当てる第２のユーザセグメントとに分割する分割手段と、

（ａ）前記第１及び第２のセッション鍵のそれぞれを、前記グループ内の各ユーザシステム固有の復号鍵に対応する公開鍵で暗号化することにより得られる複数の暗号化セッション鍵と、

（ｂ）前記第１及び第２のセッション鍵に対応する第１のベクトル（L_0，L_1，L_2，…，L_k）と、

を含み、

前記第１のベクトルは、前記グループ内の任意のユーザ識別情報ｕに関する第２のベクトル（１，ｕ，u^2，…，u^k）との内積が、$z_j u^v$（ここで、ｋは予め定められた正の整数、z_jはユーザセグメント毎に異なる複数の定数値のうち該ユーザ識別情報ｕの属するユーザセグメントに対応する定数値、ｖは前記グループにグループ識別情報として割り当てられた値に基づく「０」以上ｋ以下の整数のうちのいずれか１つの整数）に等しく

なるように設定され、

前記グループに属する各ユーザシステム固有の復号鍵を用いて、前記第１及び第２のセッション鍵のうち、当該ユーザシステムの属するユーザセグメントに割り当てられたセッション鍵が得られる暗号化セッション鍵を復号可能にするヘッダ情報を生成するヘッダ情報生成手段と、

前記第１及び第２の暗号化コンテンツと、前記ヘッダ情報を前記検査対象のユーザシステムに入力し、復号結果として、前記第１及び第２のコンテンツのうち復号されたコンテンツを取得する手段と、

前記分割手段で各ユーザセグメントに属するユーザ識別情報を変えながら前記グループを前記第１及び第２のユーザセグメントに分割し直して、前記ヘッダ情報生成手段で生成された複数のヘッダ情報と、各ヘッダ情報を前記検査対象のユーザシステムに入力したときに取得した前記復号結果との関係に基づいて、前記複数のユーザ識別情報のなかから、前記検査対象のユーザシステムがもつ１以上のユーザ識別情報を特定する特定手段と、

を備えた追跡システム。

【請求項９】

前記ヘッダ情報生成手段は、該第１のベクトルと前記第２のベクトルとの内積

【数３】

$$\sum_{i=0}^{2k'-1} L_i u^i$$

（ここで、ｋ′は不正ユーザ識別情報の数に対し予め定められた最大値であり、ｋ＝２ｋ′－１）が、$z_j\ u^{v \bmod 2k'}$に等しくなるように前記第１のベクトルを設定することを特徴とする請求項８記載の追跡システム。

【請求項１０】

各ユーザシステム固有の前記復号鍵は、

ルートのノードから１つ又は複数のノードを介して複数のリーフに至る木構造に、前記ルート、前記複数のノード及び前記複数のリーフ毎にそれぞれ異なる個別鍵生成多項式を割り当てるとともに、当該木構造上の異なる複数のリーフに、前記グループを含む複数のユーザシステムを個別に識別するための複数のユーザ識別情報の集合を分割することにより得られる複数のサブグループをそれぞれ割り当て、当該複数のサブグループのうち、当該ユーザシステムに対応するユーザ識別情報の属するサブグループに割り当てられた当該木構造上のリーフ及びその祖先ノードのそれぞれに対応する前記個別鍵生成多項式のうちの１つと、前記ルート、前記複数のノード及び前記複数のリーフで共通の共通鍵生成多項式とに、当該ユーザシステムのユーザ識別情報を代入することにより得られた値であることを特徴とする請求項８記載の追跡システム。

【請求項１１】

前記個別鍵生成多項式と前記共通鍵生成多項式の同じ次数の係数の線形和のうちの少なくとも１つは、前記木構造上の前記ルート、前記複数のノード、及び前記複数のリーフ毎にそれぞれ異なり、それ以外の前記同じ次数の係数の線形和は一定であることを特徴とする請求項１０記載の追跡システム。

【請求項１２】

前記グループ識別情報は、前記木構造上の前記ルート、前記ノード、または前記リーフの識別情報であることを特徴とする請求項３記載のコンテンツ提供システム。

【請求項１３】

前記コンテンツは、各ユーザシステム固有の復号鍵を更新するために必要な鍵更新情報であることを特徴とする請求項１記載のコンテンツ提供システム。

【請求項１４】

前記コンテンツは、前記個別鍵生成多項式の係数を更新するために必要な鍵更新情報であることを特徴とする請求項３記載のコンテンツ提供システム。

【請求項１５】
前記コンテンツは、前記個別鍵生成多項式及び前記共通鍵生成多項式の係数を更新するために必要な鍵更新情報であることを特徴とする請求項３記載のコンテンツ提供システム。
【請求項１６】
前記コンテンツは、係数群$a_{v,i}$を更新するために必要な鍵更新情報であることを特徴とする請求項５記載のコンテンツ提供システム。
【請求項１７】
前記コンテンツは、係数群$a_{v,i}$及び係数群b_iを更新するために必要な鍵更新情報であることを特徴とする請求項５記載のコンテンツ提供システム。
【請求項１８】
前記コンテンツは、係数群$a_{v,i}$、定数値λ_V、及び係数群b_iを更新するために必要な鍵更新情報であることを特徴とする請求項５記載のコンテンツ提供システム。
【請求項１９】
前記コンテンツは、前記個別鍵生成多項式A_v（ｘ）及び前記共有鍵生成多項式Ｂ（ｘ）を、新たな個別鍵生成多項式$A_{new,v}$（ｘ）及び前記共有鍵生成多項式B_{new}（ｘ）
【数４】

$$A_{new,v}(x) = \sum_{i=0}^{K_a} \{(a_{v,i} + a'_{v,i}) - \lambda_v(b_i + b'_i)\}x^i \bmod q,$$

$$B_{new}(x) = \sum_{i=0}^{K_b} (b_i + b'_i)x^i \bmod q$$

に更新するために必要な係数群$a'_{v,i}$、及び係数群b'_iを含む鍵更新情報であることを特徴とする請求項記載５記載のコンテンツ提供システム。
【請求項２０】
複数のユーザシステムを個別に識別するための複数のユーザ識別情報を複数のユーザセグメントに分割し、前記複数のユーザセグメントに対し異なる複数のセッション鍵s_j（ｊ＝１，２，…、ｎ）をそれぞれ割り当てることにより得られる、各ユーザ識別情報に対応するセッション鍵を示す情報を、当該ユーザ識別情報に対応付けて記憶するユーザ区分情報記憶手段と、
コンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化手段と、
前記暗号化コンテンツを復号するために必要なヘッダ情報を生成するヘッダ情報生成手段と、
前記暗号化コンテンツ及び前記ヘッダ情報を送信する送信手段と、
を備えたコンテンツ提供システムにおけるコンテンツ提供方法であって、
前記コンテンツ暗号化手段が、前記複数のユーザセグメントのうちの１つである第１のユーザセグメントに属するユーザ識別情報と、他の１つである第２のユーザセグメントに属するユーザ識別情報とを含む複数のユーザ識別情報のグループに対し、前記複数のセッション鍵のうち、前記第１のユーザセグメントに対応する第１のセッション鍵s_1と、前記第２のユーザセグメントに対応する第２のセッション鍵s_2とのそれぞれを用いて前記コンテンツを暗号化し、前記第１のセッション鍵に対応する第１の暗号化コンテンツと、前記第２のセッション鍵に対応する第２の暗号化コンテンツを生成するコンテンツ暗号化ステップと、
前記ヘッダ情報生成手段が、前記第１及び第２のセッション鍵のそれぞれを、前記グループ内の各ユーザシステム固有の復号鍵に対応する公開鍵で暗号化し、複数の暗号化セッション鍵を得るセッション鍵暗号化ステップと、
前記ヘッダ情報生成手段が、前記グループに対し、前記複数の暗号化セッション鍵と、前記第１及び第２のセッション鍵に対応する第１のベクトル（L_0，L_1，L_2，…，L

$_k$）とを含むヘッダ情報であって、前記第１のベクトルは、前記グループ内の任意のユーザ識別情報ｕに関する第２のベクトル（１，ｕ，ｕ^2，…，ｕ^k）との内積が、ｚ$_j$ ｕ^v（ここで、ｋは予め定められた正の整数、ｚ$_j$は前記複数のユーザセグメントに対応する異なる複数の定数値のうち該ユーザ識別情報ｕの属するユーザセグメントに対応する定数値、ｖは前記グループにグループ識別情報として割り当てられた値に基づく「０」以上ｋ以下の整数のうちのいずれか１つの整数）に等しくなるように設定され、前記グループに属する各ユーザシステムにおいて、当該ユーザシステム固有の復号鍵を用いて、前記第１及び第２のセッション鍵のうち、当該ユーザシステムの属するユーザセグメントに割り当てられたセッション鍵が得られる暗号化セッション鍵を復号可能にする前記ヘッダ情報を生成するヘッダ情報生成ステップと、

前記送信手段が、前記第１及び第２の暗号化コンテンツと、前記ヘッダ情報とを送信する送信ステップと、

を含むコンテンツ提供方法。

【請求項２１】

前記ヘッダ情報生成ステップは、前記第１のベクトルを、該第１のベクトルと前記第２のベクトルとの内積

【数５】

$$\sum_{i=0}^{2k'-1} L_i u^i$$

（ここで、ｋ′は不正ユーザ識別情報の数に対し予め定められた最大値であり、ｋ＝２ｋ′－１を満たす）が、ｚ$_j$ ｕ$^{v \bmod 2k'}$に等しくなるように設定することを特徴とする請求項２０記載のコンテンツ提供方法。

【請求項２２】

各ユーザシステム固有の前記復号鍵は、

ルートのノードから１つ又は複数のノードを介して複数のリーフに至る木構造に、前記ルート、前記複数のノード及び前記複数のリーフ毎にそれぞれ異なる個別鍵生成多項式を割り当てるとともに、当該木構造上の異なる複数のリーフに、前記グループを含む複数のユーザシステムを個別に識別するための複数のユーザ識別情報の集合を分割することにより得られる複数のサブグループをそれぞれ割り当て、当該複数のサブグループのうち、当該ユーザシステムに対応するユーザ識別情報の属するサブグループに割り当てられた当該木構造上のリーフ及びその祖先ノードのそれぞれに対応する前記個別鍵生成多項式のうちの１つと、前記ルート、前記複数のノード及び前記複数のリーフで共通の共通鍵生成多項式とに、当該ユーザシステムのユーザ識別情報を代入することにより得られた値であることを特徴とする請求項２０記載のコンテンツ提供方法。

【請求項２３】

前記個別鍵生成多項式と前記共通鍵生成多項式の同じ次数の係数の線形和のうちの少なくとも１つは、前記木構造上の前記ルート、前記複数のノード、及び前記複数のリーフ毎にそれぞれ異なり、それ以外の前記同じ次数の係数の線形和は一定であることを特徴とする請求項２２記載のコンテンツ提供方法。

【請求項２４】

コンテンツを暗号化して暗号化コンテンツを生成するコンテンツ暗号化手段と、

前記暗号化コンテンツを復号するために必要なヘッダ情報を生成するヘッダ情報生成手段と、

制御手段と、

を備え、検査対象のユーザシステムを検査し、複数のユーザシステムを個別に識別するための複数のユーザ識別情報のなかから不正ユーザ識別情報を特定するための追跡システムにおける不正ユーザ特定方法であって、

（ａ）前記コンテンツ暗号化手段が、第１のセッション鍵ｓ$_1$と第２のセッション鍵ｓ$_2$

とを用いて、異なる電子透かし情報が埋め込まれている第１及び第２のコンテンツをそれぞれ暗号化し、前記第１のセッション鍵で復号可能な第１の暗号化コンテンツと前記第２のセッション鍵で復号可能な第２の暗号化コンテンツを得、前記検査対象のユーザシステムに入力するコンテンツ暗号化ステップと、

（ｂ）前記制御手段が、複数のユーザ識別情報を含むグループを、前記第１のセッション鍵を割り当てる第１のユーザセグメントと、前記第２のセッション鍵を割り当てる第２のユーザセグメントとに分割する分割ステップと、

（ｃ）前記ヘッダ情報生成手段が、前記第１及び第２のセッション鍵のそれぞれを、前記グループ内の各ユーザシステム固有の復号鍵に対応する公開鍵で暗号化することにより得られる複数の暗号化セッション鍵と、前記第１及び第２のセッション鍵に対応する第１のベクトル（L_0，L_1，L_2，…，L_k）とを含むヘッダ情報であって、前記第１のベクトルは、前記グループ内の任意のユーザ識別情報ｕに関する第２のベクトル（１，ｕ，u^2，…，u^k）との内積が、$z_j u^v$（ここで、ｋは予め定められた正の整数、z_jはユーザセグメント毎に異なる複数の定数値のうち該ユーザ識別情報ｕの属するユーザセグメントに対応する定数値、ｖは前記グループにグループ識別情報として割り当てられた値に基づく「０」以上ｋ以下の整数のうちのいずれか１つの整数）に等しくなるように設定され、前記グループに属する各ユーザシステムにおいて、当該ユーザシステム固有の復号鍵を用いて、前記第１及び第２のセッション鍵のうち、当該ユーザシステムの属するユーザセグメントに割り当てられたセッション鍵が得られる暗号化セッション鍵を復号可能にするヘッダ情報を生成するヘッダ情報生成処理を実行するステップと、

（ｄ）前記ヘッダ情報生成手段が、前記ヘッダ情報生成処理で生成されたヘッダ情報を前記検査対象のユーザシステムに入力するステップと、

（ｅ）前記制御手段が、前記第１及び第２の暗号化コンテンツと、前記ヘッダ情報とが入力された前記検査対象のユーザシステムから、復号結果として、前記第１及び第２のコンテンツのうち復号されたコンテンツを取得するステップと、

（ｆ）前記制御手段が、各ユーザセグメントに属するユーザ識別情報を変えて前記グループを前記第１及び第２のユーザセグメントに分割し直すステップと、

（ｇ）前記ヘッダ情報生成手段が、前記ヘッダ情報生成処理を実行するステップと、

（ｈ）前記ヘッダ情報生成手段が、前記ヘッダ情報生成処理で生成された新たなヘッダ情報を前記検査対象のユーザシステムに入力するステップと、

（ｉ）前記制御手段が、前記新たなヘッダ情報が入力された前記検査対象のユーザシステムから新たな復号結果を取得するステップと、

（ｊ）前記（ｆ）～前記（ｉ）を複数回繰り返すことにより前記ヘッダ情報生成手段で生成された複数の前記ヘッダ情報と複数の前記復号結果との関係に基づいて、前記制御手段が、前記複数のユーザ識別情報のなかから、前記検査対象のユーザシステムがもつ１以上のユーザ識別情報を特定する特定ステップと、

を含む不正ユーザ特定方法。

【請求項２５】

前記ヘッダ情報生成処理は、該第１のベクトルと前記第２のベクトルとの内積

【数６】

$$\sum_{i=0}^{2k'-1} L_i u^i$$

（ここで、ｋ′は不正ユーザ識別情報の数に対し予め定められた最大値であり、ｋ＝２ｋ′－１）が、$z_j u^{v \bmod 2k'}$に等しくなるように前記第１のベクトルを設定することを特徴とする請求項２４記載の不正ユーザ特定方法。

【請求項２６】

前記コンテンツは、各ユーザシステム固有の復号鍵を更新するために必要な鍵更新情報であることを特徴とする請求項２０記載のコンテンツ提供方法。

【請求項２７】
前記コンテンツは、前記個別鍵生成多項式の係数を更新するために必要な鍵更新情報であることを特徴とする請求項２２記載のコンテンツ提供方法。
【請求項２８】
前記コンテンツは、前記個別鍵生成多項式及び前記共通鍵生成多項式の係数を更新するために必要な鍵更新情報であることを特徴とする請求項２２記載のコンテンツ提供方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンテンツ提供システムから複数のユーザシステムへ、暗号化コンテンツと、当該暗号化コンテンツを復号するためのヘッダ情報を送信するデータ通信システムに関する。
【背景技術】
【０００２】
従来、放送型コンテンツ配信事業では、放送番組のコンテンツを暗号化し、得られた暗号化コンテンツをユーザに配信する。ユーザは、例えば配信者から貸与された正当な復号器により暗号化コンテンツを復号し、得られたコンテンツにより放送番組を視聴している。しかしながら、放送型コンテンツ配信事業に対しては、自己の正当な復号器の内部情報（復号鍵等）をコピーした海賊版復号器（不正復号器）を作成し、暗号化コンテンツを不正に復号可能とする不正ユーザが存在している。
【０００３】
一方、このような不正ユーザを特定し得る各種の不正ユーザ特定方法が知られている。係る不正ユーザ特定方法は、ユーザの復号鍵生成方法により三つのタイプに分類される。第１のタイプは、組み合わせ論的な構成に基づく方法であり、第２のタイプは、木構造に基づく方法であり、第３のタイプは、代数的な構成に基づく方法である。
【０００４】
第１のタイプでは、不正復号器の作成に関与しない正当なユーザを不正ユーザと誤って検出する確率を十分小さくするために送信オーバヘッドを非常に大きくしなければならない問題がある。
【０００５】
第２及び第３のタイプでは、この問題を解決し、効率的な送信オーバヘッドを達成している。
【０００６】
しかしながら、不正復号器は、複数の不正ユーザの結託により、複数の復号鍵または復号鍵と等価な機能をもつデータが格納されることがある。この不正復号器に対して、不正復号器をこじ開けずにその入出力のみを観測し、不正ユーザを特定するブラックボックス追跡が行なわれる場合がある。具体的には、ブラックボックス追跡を行う追跡者は、不正ユーザの候補（以下、容疑者という）を想定し、容疑者の復号鍵が不正復号器に保持されているか否かを、不正復号器への入出力を観測することのみにより検査する。
【０００７】
第２及び第３のタイプの不正ユーザ特定方法では、下記二つの問題のいずれかが未解決である。
【０００８】
問題１：ブラックボックス追跡の際に、各入力の意図（想定した容疑者）が不正復号器に知られてしまうため、巧妙な不正復号器が入力の意図を読み取って不正ユーザの特定を妨げるように動作した場合、ブラックボックス追跡が失敗する。この失敗は、不正ユーザを特定できないか、または無実のユーザに濡れ衣を着せてしまう問題につながる。
【０００９】
問題２：不正復号器が入力の意図を読み取ることは不可能であるが、不正ユーザを正しく特定する確率が送信オーバヘッドとトレードオフの関係にあり、送信オーバヘッドを効

率的にすると不正ユーザを正しく特定する確率が非常に低くなるという問題、またはブラックボックス追跡に要する処理ステップ数が指数関数的であり、かかるブラックボックス追跡は、全ユーザ数をｎ、最大結託人数をｋとしたとき、ｎＣｋ＝ｎ！／｛ｋ！（ｎ－ｋ）！｝通りの容疑者集合を検査する必要があるため、実用上不可能となる問題がある。

【００１０】

以上説明したように従来の不正ユーザ特定方法では、巧妙な不正復号器に対しては、不正ユーザを特定に失敗するという問題点がある。このような問題点を解決するために、非特許文献１では、不正ユーザ特定のためのブラックボックス追跡の際に、入力の意図を不正復号器に知られることが無く、巧妙な不正復号器に対しても、確実に追跡を実行し得る不正ユーザ特定方法が開示されている。

【００１１】

非特許文献１において開示されている不正ユーザ特定方法は、より効率的な送信オーバヘッドを達成しているが、過去の入力を記憶できる、より巧妙な不正復号器を対象とするものではない。不正復号器が過去の入力を記憶できる、より巧妙な不正復号器の場合、それを利用して現在の入力の意図が推測される可能性がある。すなわち、非特許文献１の不正ユーザ特定方法では、不正復号器が過去に与えられた入力を記憶しないという仮定を置く必要がある。例えば、不正復号器がソフトウェア（プログラム）により実装されている場合、プログラムのコピーを検査回数分作成しておき、各検査において異なる（コピーされた）プログラムを用い、１つのプログラムに与える入力を１回のみにすれば、不正復号器が過去の入力を記憶することはないため、上記仮定の下で不正ユーザの特定を行うことができる。

【００１２】

しかしながら、過去の入力を記憶し、それに基づいて不正ユーザの特定を妨げるように動作する、さらに巧妙な不正復号器に対してもブラックボックス追跡を行うことができることが望ましい。

【００１３】

過去の入力を記憶する不正復号器に対する不正ユーザ特定方法が非特許文献２に開示されているが、この方法は上記第１タイプであるため、送信オーバヘッドを非常に大きくしなければならないという問題点がある。このような不正復号器を対象とする不正ユーザ特定方法においても、送信オーバヘッドを削減することが望ましい。また、不正ユーザが特定された後、不正ユーザをシステムから完全に排除するために、復号鍵の更新を行えることが望ましい。

【非特許文献１】松下、今井：より強力な不正者に対する効率的なブラックボックス追跡のための階層的な鍵割り当て、電子情報通信学会 情報セキュリティ研究会、ISEC2006-52、pp.91-98、2006年7月。

【非特許文献２】A. Kiayias and M. Yung, “On Crafty Pirates and Foxy Tracers,” Security and Privacy in Digital Rights Management: Revised Papers from the ACM CCS-8 Workshop DRM 2001, LNCS 2320, pp.22-39, Springer-Verlag, 2002.

【発明の開示】

【発明が解決しようとする課題】

【００１４】

以上説明したように従来の不正ユーザ特定方法では、不正ユーザを特定するために不正復号器に入力された入力データを記憶し、記憶した入力データに基づき不正ユーザの特定を妨げるように動作する巧妙な不正復号器からは、少ない送信オーバヘッドで不正ユーザを特定することができないという問題点があった。

【００１５】

そこで、本発明は上記問題点に鑑み、少ない送信オーバヘッドで、より巧妙な不正復号器からも不正ユーザを特定することが確実に行えるコンテンツ提供システム及び追跡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】

【００１６】
コンテンツ提供システムは、
異なる複数のセッション鍵s_j（ｊ＝１，２，…、ｎ）を用いてコンテンツを暗号化し、複数の暗号化コンテンツを得るコンテンツ暗号化手段と、
前記複数のセッション鍵のそれぞれを、各ユーザシステム固有の復号鍵に対応する公開鍵で暗号化し、複数の暗号化セッション鍵を得るセッション鍵暗号化手段と、
前記複数のセッション鍵が割り当てられた、複数のユーザシステムを個別に識別するための複数のユーザ識別情報を含むグループに対し、
（ａ）前記複数の暗号化セッション鍵と、
（ｂ）前記複数のセッション鍵のうち前記グループ内の任意のユーザ識別情報ｕに割り当てられているセッション鍵に対応する第１のベクトル（L_0，L_1，L_2，…，L_k）と、該ユーザ識別情報ｕに関する第２のベクトル（１，ｕ，u^2，…，u^k）との内積が、$z_j\ u^v$（ここで、ｋは予め定められた正の整数、z_jは前記複数のセッション鍵に対応する異なる複数の定数値のうち該ユーザ識別情報ｕに割り当てられているセッション鍵s_jに対応する定数値、ｖは前記グループにグループ識別情報として割り当てられた「０」以上ｋ以下の整数のうちのいずれか１つの整数）に等しくなるように設定された前記第１のベクトルと、
を含み、前記グループに属する各ユーザシステム固有の復号鍵を用いて各ユーザシステムに割り当てられた暗号化セッション鍵を復号可能にするヘッダ情報を生成するヘッダ情報生成手段と、
前記複数の暗号化コンテンツのうちの少なくとも１つ及び前記ヘッダ情報を前記複数のユーザシステムへ送信する送信手段と、
を含む。
【発明の効果】
【００１７】
本発明によれば、少ない送信オーバヘッドで、より巧妙な不正復号器からも不正ユーザを特定することが確実に行える。
【発明を実施するための最良の形態】
【００１８】
以下、本発明の各実施形態について図面を参照しながら説明する。
（第１の実施形態）
図１は本発明の第１の実施形態に係るコンテンツ提供システム及びユーザシステム等が適用されたデータ通信システムの構成を示す模式図であり、図２及び図３は同実施形態におけるユーザ識別情報のサブグループを説明するための模式図であり、図４は同実施形態における追跡システムの構成を示す模式図である。
【００１９】
このデータ通信システムは、図１に示すように、暗号化装置１０と電子透かし埋め込み装置１０１を含むコンテンツ提供システム１と、復号装置２０を有するｎ個のユーザシステム２とがネットワーク３を介して接続されている。また、ネットワーク３には例えば追跡装置３０が接続されている。
【００２０】
ここで、コンテンツ提供システム１は、コンテンツを暗号化してネットワーク３を介してブロードキャストあるいはマルチキャストするものである。
【００２１】
ｎ個のユーザシステム２は、コンテンツ提供システム１によりブロードキャストあるいはマルチキャストされた暗号化コンテンツをネットワーク３を介して受信し復号するものである。
【００２２】
なお、図１では、１つのコンテンツ提供システム１のみ示しているが、コンテンツ提供システム１が複数存在しても構わない。

【００２３】
また、１つのノードが、コンテンツ提供システム１の機能とユーザシステム２の機能とを兼ね備えてもよい。また、全てのノードがコンテンツ提供システム１の機能とユーザシステム２の機能とを兼ね備えることによって、相互に暗号通信可能としてもよい。
【００２４】
電子透かし埋め込み装置１０１は、図１に示すように、コンテンツ提供システム１内にあってもよいし、暗号化装置１０が電子透かし埋め込み機能を有していてもよい。電子透かしの埋め込まれたコンテンツをコンテンツ暗号化部１４が暗号化するような構成であれば、電子透かし埋め込み機能はどこにあってもよい。電子透かしの埋め込まれたコンテンツが第三者装置からコンテンツ提供システムへ与える構成であってもよい。
【００２５】
ネットワーク３は、有線ネットワークでも、無線ネットワークでもよい。また、有線ネットワークと無線ネットワークを両方使用したものであってもよい。また、双方向ネットワークでも、単方向ネットワークでもよい。また、ネットワーク３は、オフラインであってもよい。つまりＤＶＤ等の媒体を用いて実現されていても構わない。
【００２６】
次に、電子透かし埋め込み装置１０１と暗号化装置１０について説明する。
【００２７】
電子透かし埋め込み装置１０１は、ユーザ区分管理部１２からの情報（電子透かし情報がいくつ必要かなど）に基づき、入力されたコンテンツに各電子透かし情報を埋め込み、異なる電子透かしの埋め込まれた複数の電子透かし入りコンテンツを出力する。電子透かし埋め込み装置１０１は、電子透かし情報を人間に知覚されない範囲で、入力されたコンテンツに埋め込む。一旦電子透かし情報の埋め込まれたコンテンツからは該電子透かし情報を除去または改ざんすることは非常に困難である。電子透かし埋め込み装置１０１は、例えば、参考文献１（I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “A Secure, Robust Watermark for Multimedia,” Proc. Information Hiding, LNCS 1174, pp.185-206, Springer-Verlag, 1996.）に開示されているような公知の方法を用いて電子透かしの埋め込みを行う。
【００２８】
例えば、２つの異なる電子透かし情報Ａ、Ｂを、入力されたコンテンツに埋め込む場合、電子透かし埋め込み装置１０１からは、電子透かし情報Ａが埋め込まれた第１のコンテンツと電子透かし情報Ｂが埋め込まれた第２のコンテンツが出力される。なお、異なる３つ以上の電子透かし情報がそれぞれ埋め込まれた複数の（３つ以上の）コンテンツを出力するようにしてもよい。また、図１５（ａ）に示すように、コンテンツの複数の箇所に電子透かし情報を埋め込み、電子透かし情報の埋め込まれたコンテンツの全体を出力してもよい。さらに、図１５（ｂ）に示すように、コンテンツの複数の箇所に電子透かし情報を埋め込み、コンテンツ全体のうち、電子透かし情報の埋め込まれた該コンテンツの一部分（図１５（ｂ）の点線部分）を出力し、電子透かし情報の埋め込まれていない部分の出力を省略してもよい。
【００２９】
暗号化装置１０は、公開鍵格納部１１、ユーザ区分管理部１２、セッション鍵生成部１３、コンテンツ暗号化部１４、ヘッダ生成部１５及びユーザ区分情報格納部１６を備えている。
【００３０】
公開鍵格納部１１は、公開鍵を格納するメモリであり、セッション鍵生成部１３及びヘッダ生成部１５から読出可能となっている。
【００３１】
ユーザ区分情報格納部１６は、複数のユーザシステム２を個別に識別するための複数のユーザ識別情報のそれぞれに対し、複数のセッション鍵のうち、該ユーザ識別情報に対応するユーザシステムで復号可能なセッション鍵を示す情報や、無効化対象ユーザであるか

否かを示す情報などを記憶するメモリである。本実施形態では、複数のユーザ識別情報を複数のユーザセグメントに分割し、該複数のユーザセグメントには、異なる複数のセッション鍵をそれぞれ対応付ける。複数のセッション鍵は、埋め込まれている電子透かし情報がそれぞれ異なる複数のコンテンツに、それぞれ対応する。

【００３２】

ユーザ区分管理部１２は、上記ユーザセグメントに関する情報や無効化対象ユーザに関する情報を含むユーザ区分情報が外部から入力されると、該ユーザ区分情報をユーザ区分情報格納部１６に記憶する。また、ユーザ区分管理部１２は、ユーザ区分情報格納部１６に格納されている情報を基に、ヘッダ生成部１５、セッション鍵生成部１３、及び電子透かし埋め込み装置１０１に対し、必要な情報を出力する。

【００３３】

セッション鍵生成部１３は、公開鍵格納部１１内の公開鍵をもとに複数のセッション鍵を生成する。

【００３４】

コンテンツ暗号化部１４は、電子透かし埋め込み装置１０１より得られる、異なる複数の電子透かし情報がそれぞれ埋め込まれた複数のコンテンツを、セッション鍵生成部１３により生成されたセッション鍵に基づいてそれぞれ暗号化し、複数の暗号化コンテンツを生成する。なお、各暗号化コンテンツは対応するセッション鍵に基づいて復号可能である。

【００３５】

ヘッダ生成部１５は、公開鍵、セッション鍵（のもととなる情報）、（無効化対象ユーザがある場合には）無効化対象ユーザ情報や、その他の必要なパラメータ（後述する例では、パラメータｐ、ｑ、ｋ、Ｔ）等に基づいてヘッダ情報を生成する。

【００３６】

具体的には、ヘッダ生成部１５は、暗号化セッション鍵及び２種類のヘッダ情報を生成する。暗号化セッション鍵は、セッション鍵を公開鍵で暗号化することにより、生成される。

【００３７】

第１のヘッダ情報は、対応付けられているセッション鍵がそれぞれ異なる複数のユーザセグメントに属するユーザシステムが混在するグループに対応する。すなわち、該グループには、異なる複数の電子透かし情報のうちの１つの電子透かし情報が埋め込まれたコンテンツが得られる（ユーザ識別情報をもつ）ユーザシステム、他の１つの電子透かし情報が埋め込まれたコンテンツが得られる（ユーザ識別情報をもつ）ユーザシステムが混在し、さらに他の電子透かし情報が埋め込まれたコンテンツが得られる（ユーザ識別情報をもつ）ユーザシステムが含まれている。

【００３８】

第１のヘッダ情報は、（ａ）各セッション鍵を公開鍵で暗号化して得られた複数の暗号化セッション鍵を含み、且つ（ｂ）該グループ内の任意のユーザ識別情報ｕに割り当てられているセッション鍵に対応する第１のベクトル（L_0，L_1，L_2，…，L_k）とを含む。

【００３９】

この第１のベクトルは、該第１のベクトルと、該ユーザ識別情報ｕに関する第２のベクトル（１，ｕ，u^2，…，u^k）との内積が、$z_j\ u^v$に等しくなるように設定されている。ここで、予め定められた正の整数をｋ、複数のセッション鍵に対応する異なる複数の定数値のうち該ユーザ識別情報ｕに割り当てられているセッション鍵s_jに対応する定数値をz_j、該グループにグループ識別情報として割り当てられた、「０」以上ｋ以下の整数のうちのいずれか１つの整数をｖとする。

【００４０】

特に、不正ユーザ識別情報の数に対し予め定められた最大値（最大結託人数）がｋ´であり、ｋとｋ´とがｋ＝２ｋ´－１を満たす場合、第１のベクトルと第２のベクトルとの

内積
【数７】

$$\sum_{i=0}^{2k'-1} L_i u^i$$

【００４１】
が、ｚｕ$^{v \bmod 2k'}$に等しくなるように、該第１のベクトルが設定されている。
【００４２】
なお、暗号化セッション鍵は、各ユーザシステム固有の復号鍵に基づいて復号可能であり、該ユーザシステムが、どのユーザセグメントに属するか（どのセッション鍵が割り当てられているユーザセグメントに属するか）によって、復号できるセッション鍵は異なる。
【００４３】
第２のヘッダ情報は、ある１つのセッション鍵が割り当てられているユーザセグメントに属するユーザシステムのみを含むグループに対応する。すなわち、該グループに属するユーザシステムは、同一の電子透かし情報が埋め込まれたコンテンツを得る。第２のヘッダ情報は、該セッション鍵を公開鍵で暗号化して得られた暗号化セッション鍵を含む。なお、第２のヘッダ情報は、上述した値L_iに基づく値を含まない。但し、第２のヘッダ情報は、上述した値L_iに基づく値を含んでもよい。
【００４４】
なお、コンテンツ提供システム１は、ヘッダ情報及び暗号化コンテンツの通信インタフェース、コンテンツを蓄積する装置、コンテンツを入力する装置あるいは復号鍵生成装置（図示せず）など、種々の装置を必要に応じて備えるものとする。また、コンテンツ提供システム１は、ユーザシステムに各ヘッダ情報を送信するとき、データ量を低減させる観点から、各ヘッダ情報の共通部分を共有化して送信することが好ましい。但し、これに限らず、共通部分を共有化しなくてもよい。
【００４５】
ここで、復号鍵生成装置は、各ユーザシステム固有の復号鍵を生成するものであり、複数のユーザシステムを個別に識別するための複数のユーザ識別情報を複数のサブグループに分割し、木構造化する機能と、サブグループ毎に互いに異なる鍵生成多項式と共通の鍵生成多項式を割り当てる機能と、ユーザシステム毎のユーザ識別情報をこのユーザ識別情報が属するサブグループの鍵生成多項式に代入し、得られた値を当該ユーザシステム固有の復号鍵とする機能とをもっている。
【００４６】
詳しくは、ユーザの復号鍵は鍵生成多項式にユーザ識別情報、すなわち、ユーザＩＤ（一定の範囲内から選択された正整数（例えば、１からｎまでの連番）とする）を代入して生成する。その際、図１３に示すように、ユーザ集合Ｕを複数のサブグループに分割し、各サブグループを木構造のリーフに割り当てる。図１３は、全リーフ数が８である完全二分木の例である。以下、全リーフ数をＬ、木の深さをＤ、各サブグループがどのリーフに割り当てられているかの情報や各ノードＩＤを含めた木構造をＴと表す。
【００４７】
図１３に示すように、木構造Ｔでは、各ノードにＩＤ（ここでは、「０」「１」「２」…「１３」）が割り振られている。あるノードｖを祖先に持つリーフに割り振られたユーザ集合をU_vとする。なお、祖先の語は、ルートのノードに限らず、親ノード、又は親の親ノード、又は親の親の親ノード…を意味する。図１３では、例えば、$U_8 = U_0 + U_1$である。ここで、＋は和集合を表す。図１３において、全ユーザ集合ＵをサブグループU_0、…U_7に分割する。
【００４８】
図２は、サブグループU_1、U_2、U_3の一例である。図３に示すように、ユーザ集合を

複数のサブグループに分割し、各サブグループへの鍵生成多項式の割り当て方を以下のようにする。

【００４９】

例えばサブグループU_1に対しては、

A_1（ｘ）、Ｂ（ｘ）を割り当てる。

サブグループU_2に対しては、

A_2（ｘ）、Ｂ（ｘ）を割り当てる。

サブグループU_3に対しては、

A_3（ｘ）、Ｂ（ｘ）を割り当てる。

【００５０】

以下同様にして、サブグループU_iに対しては、A_i（ｘ）、Ｂ（ｘ）を割り当てる。

【００５１】

ここで、A_i（ｘ）はサブグループU_i（言い換えるとノードｉ）に固有な鍵生成多項式（個別鍵生成多項式）であり、Ｂ（ｘ）は各サブグループ（言い換えると各ノード）に共通の鍵生成多項式（共通鍵生成多項式）である。なお、上記割り当て方は一例であり、例えば、鍵生成多項式A_i（ｘ）をサブグループ番号ｉに対応させずランダムかつユニークに割り当てる割り当て方も可能であるし、どのサブグループにも割り当てられない鍵生成多項式A_j（ｘ）が存在してもよい。

【００５２】

このように、それぞれのサブグループに対し異なる鍵生成多項式とそれぞれのサブグループに対し共通の鍵生成多項式を割り当て、当該ユーザＩＤの属するサブグループに割り当てられた鍵生成多項式を用いて当該ユーザＩＤの復号鍵を生成するようにする。ここで、当該ユーザＩＤの属するサブグループ数は（ルートを除いて）Ｄであることに注意する。例えば、図１３において、リーフ０に割り当てられたユーザは、サブグループU_8、U_{12}にも属しており、それぞれのサブグループに割り当てられる鍵生成多項式を用いて当該ユーザＩＤの復号鍵が生成される。

【００５３】

これにより、従来のブラックボックス追跡方法では、鍵生成多項式A_i（ｘ）、B_i（ｘ）の両方ともノードに対し異なる鍵生成多項式であったのに対して、後述するように、本発明では、一方の鍵生成多項式Ｂ（ｘ）をノードに対し共通としても、巧妙な不正復号器に対するブラックボックス追跡が可能となる鍵生成多項式を導入することにより、復号器が保持すべき復号鍵データサイズを半分弱程度削減可能となる。

【００５４】

なお、ユーザシステム２に割り当てられたユーザＩＤを、当該ユーザＩＤの属するサブグループに割り当てられた鍵生成多項式に代入して得られる復号鍵は、予めコンテンツ提供システム１または信頼できる第三者からユーザシステム２へ与えられて保持しておくものとする。

【００５５】

なお、図１３、図２、及び図３に例示したグルーピングの方法は一例であり、この他にも種々のグルーピングの仕方が可能である。

【００５６】

また、上記では、ユーザＩＤやノードＩＤを一定の範囲内から選択された正整数（例えば、１からｎまでの連番）としているが、その代わりに、ユーザＩＤは特に正整数とはせずに（例えば、英数字等でもよい）、英数字等のユーザＩＤに対して固有に一定の範囲内から選択された正整数を割り当て、ユーザＩＤに固有に割り当てられた正整数及び該当する鍵生成多項式をもとに復号鍵を計算する構成も可能である。ノードＩＤについても同様である。

【００５７】

次に、ユーザシステム２に搭載される復号装置２０を説明する。

復号装置２０は、図１に示すように、ユーザ情報格納部２１、セッション鍵復号部２２

及びコンテンツ復号部２３を備えている。

【００５８】

ユーザ情報格納部２１は、復号に必要なパラメータ（後述する例では、パラメータｐ、ｑ、ｋ）と、自システム２が属するサブグループＩＤと、自システム２に割り当てられたユーザＩＤと、該ユーザＩＤに対応する復号鍵とを格納するメモリであり、セッション鍵復号部２２から読出可能となっている。なお、復号鍵は、該ユーザＩＤが属するサブグループに割り当てられた鍵生成多項式に該ユーザＩＤを代入することによって得られる値である。

【００５９】

セッション鍵復号部２２は、コンテンツ提供システム１から暗号化コンテンツとヘッダ情報とを受信したとき、ユーザ情報格納部２１内の復号鍵に基づいて、ヘッダ情報からセッション鍵を取得（復号）する。

【００６０】

コンテンツ復号部２３は、セッション鍵復号部２２により取得（復号）したセッション鍵に基づいて、コンテンツ提供システム１から受信した暗号化コンテンツを復号する。

【００６１】

なお、ユーザシステム２は、コンテンツ提供システム１から暗号化コンテンツとヘッダ情報とを受信する通信インタフェース、コンテンツを蓄積する装置あるいはコンテンツを表示等する装置など、種々の装置を必要に応じて備えるものとする。

【００６２】

次に、図４を用いて追跡装置３０を説明する。

追跡装置３０は、公開鍵格納部３１、ヘッダ生成部３２、電子透かし埋め込み部３４、コンテンツ暗号化部３５及び制御部３３を備えている。なお、電子透かし埋め込み部３４は、必ずしも追跡装置３０の中に含まれている必要はなく、コンテンツ暗号化部３５が、電子透かし情報の埋め込まれているコンテンツを暗号化するような構成であれば、電子透かし埋め込み機能は、どこにあってもよい。追跡装置３０の外部にある装置から、電子透かしの埋め込まれたコンテンツがコンテンツ暗号化部３５に入力される構成であってもよい。

【００６３】

コンテンツ暗号化部３５には、異なる複数の電子透かし情報がそれぞれ埋め込まれた複数種類のコンテンツが入力される。

【００６４】

コンテンツ暗号化部３５は、上記複数種類のコンテンツのそれぞれを、該コンテンツに対応するセッション鍵を用いてそれぞれ暗号化して、複数の暗号化コンテンツを生成する機能と、該複数の暗号化コンテンツを検査対象に入力する機能とをもっている。前述のコンテンツ提供システムと同様、上記複数種類のコンテンツには、異なる複数のセッション鍵がそれぞれ対応付けられている。また、複数のセッション鍵は、複数のユーザセグメントにそれぞれ割り当てられている。

【００６５】

公開鍵格納部３１は、公開鍵を格納するメモリであり、ヘッダ生成部３２から読出可能となっている。

【００６６】

ヘッダ生成部３２は、制御部３３から指示された、各ユーザ識別情報（各ユーザシステム）が属するユーザセグメントに従い、公開鍵やその他の必要なパラメータ（後述する例では、パラメータｐ、ｑ、ｋ、Ｔ等をもとにしてヘッダ情報を生成する機能と、ヘッダ情報を検査対象に入力する機能とをもっている。なお、セッション鍵（のもととなる情報）は、制御部３３が生成してヘッダ生成部３２に指示してもよいし、ヘッダ生成部３２が生成して制御部３３に通知してもよい。また、ヘッダ情報は、前述した値L_iに基づく値を含むように生成される。

【００６７】

制御部（特定手段）３３は、追跡装置３０全体の制御を司るものであり、ヘッダ生成部３２により、例えば複数のユーザセグメントのうちのある１つのユーザセグメントについて、該ユーザセグメントに属するユーザシステムの数を「０」から１つずつ増やしながら生成された複数のヘッダ情報と、各ヘッダ情報を入力したときに取得した復号結果との関係に基づいて、前記検査対象のユーザシステムの作出のもととなった１又は複数のユーザシステムの不正ユーザ（ユーザ識別情報）を特定する機能をもっている。

【００６８】

例えば、制御部３３は、電子透かし情報Ａが埋め込まれた第１のコンテンツを復号可能なユーザ識別情報（ユーザシステム）の集合（第１のユーザセグメントχ_1）や、電子透かし情報Ｂが埋め込まれた第２のコンテンツを復号可能なユーザ識別情報（ユーザシステム）の集合（第２のユーザセグメントχ_2）をヘッダ生成部３２に指示する機能と、検査対象復号装置２０χで復号されたコンテンツを入力し、それが第１のコンテンツであるか第２のコンテンツであるかを調べる機能と、第１のユーザセグメントχ_1に属するユーザ識別情報を１つずつ増やしながら、同様の処理を繰り返し行い、それらの判定結果を総合して、不正ユーザのユーザ識別情報を特定する機能とをもっている。

【００６９】

制御部３３は、検査対象復号装置２０χに入力した複数種類の暗号化コンテンツのうちどの暗号化コンテンツが復号されたか（例えば電子透かし情報Ａ及びＢのうちどちらの電子透かし情報が埋め込まれているコンテンツであるか）を基に、不正ユーザのユーザ識別情報を特定する。しかし、この場合に限らず、セッション鍵自体がコンテンツである場合、セッション鍵のみを検査対象復号装置２０χに入力し、検査対象復号装置２０χによるセッション鍵の復号結果（どの透かし情報が埋め込まれているか）を判断してもよい。

【００７０】

追跡装置３０は、例えば、コンテンツ提供システム１に含まれていてもよいし、図１に示したように、コンテンツ提供システム１とは独立した装置で、ネットワーク３に接続する機能を備えてもよい。追跡装置３０は、必ずしもネットワーク３に接続する機能を備える必要はない。

【００７１】

次に、以上のように構成されたネットワーク通信システムの動作を説明する。図５は同システムの全体動作を説明するためのフローチャートである。

【００７２】

各ユーザシステム２には、それぞれ固有のユーザ識別情報（ユーザＩＤ）が割り当てられているとする。

【００７３】

コンテンツ提供システム１は、複数のセッション鍵ｓ１,ｓ２、…ｓｊを生成し（ステップＳＴ１）、電子透かし情報ｉ（ｉ＝１、２、…、ｊ）が埋め込まれているコンテンツを得るユーザセグメントχｉに応じてセッション鍵ｓｉ（ｉ＝１、２、…、ｊ）を暗号化し、ヘッダ情報Ｈ（χ）を生成する（ステップＳＴ２）。

【００７４】

次に、コンテンツ提供システム１は、セッション鍵ｓｉで、電子透かし情報ｉが埋め込まれたコンテンツを暗号化し（ステップＳＴ３）、得られた暗号化コンテンツに、上記ヘッダ情報を付加してブロードキャストあるいはマルチキャストする（ステップＳＴ４）。

【００７５】

なお、ステップＳＴ２、ＳＴ３は、上記とは逆の順序で行ってもよいし、同時に行ってもよい。また、セッション鍵をその都度変更しない場合は、ステップＳＴ１が省かれることもある（従前のセッション鍵を使用する）。

【００７６】

各々のユーザシステム２は、ヘッダ情報／暗号化コンテンツを受信すると、自己のユーザＩＤ及びサブグループＩＤに基づき、電子透かし情報ｉが埋め込まれたコンテンツを得るユーザセグメントχｉとの関係に応じて、ヘッダ情報を復号処理する（ステップＳＴ５

）。すなわち、ユーザシステム２は、電子透かし情報ｉが埋め込まれたコンテンツを得るユーザセグメントχｉに属していれば、ステップＳＴ５の復号処理において、セッション鍵ｓｉを取得し（ステップＳＴ６）、該セッション鍵ｓｉで暗号化コンテンツを復号する（ステップＳＴ７）。

【００７７】

また、詳しくは後述するように、コンテンツ提供システム１は、電子透かし情報ｉが埋め込まれたコンテンツを得るユーザセグメントχｉに応じてヘッダ情報を生成するので、どのユーザがどの電子透かし情報が埋め込まれたコンテンツを得るかを柔軟に制御できる。

【００７８】

次に、予め実行される鍵生成フェーズ、ステップＳＴ２の暗号化フェーズ、ステップＳＴ５～ＳＴ６の復号フェーズについて、詳細に説明する。

【００７９】

始めにパラメータを定義する。

全ユーザ数をｎとし、最大結託人数をｋとする。

ｐ、ｑを素数とし、ｑはｐ－１を割り切り、かつ、ｑはｎ＋２ｋ－１以上であるとする。

【００８０】

Ｚｑ＝｛０、１、…、ｑ－１｝とする。

Zp^{*}＝｛１、…、ｐ－１｝とする。

Ｇｑを、Zp^{*}の部分群であり、かつ、位数がｑである乗法群とし、ｇをＧｑの生成元とする。

全ユーザのユーザＩＤ（ユーザ識別情報）の集合（以下、ユーザ集合という）を、Ｕ（Ｕ⊆Ｚｑ－｛０｝）とする。なお、Ｚｑ－｛０｝は、Ｚｑから｛０｝を取り除いたものを意味する。

ｐ、ｑ、ｇの値は公開されている。

以下、特に断りの無い限り、計算はZp^{*}上で行われるとする。なお、Ｇｑとして、上記の例に限らず、例えば、楕円曲線上の点から成る加法群を用いてもよい。これは以下の各実施形態でも同様である。

【００８１】

（鍵生成フェーズ）

本実施形態では、複数のユーザシステムを個別に識別するための複数のユーザＩＤを含むユーザ集合Ｕ（ユーザグループ）を、複数のサブグループに分割する。そして、各サブグループをリーフ（leaf；葉）に割り当てた二分木構造を用いる。具体的には、二分木構造のルート（root；根）から複数のノード（node；節）を介して複数のリーフに至るまでの各ノードにそれぞれ鍵生成多項式を割り当てる。これにより、鍵生成多項式をマルチレベルに階層化した例である。なお、以下の例では、二分木構造を用いた例を説明しているが、これに限らず、分岐数はいくつでもよいし、１つの木構造の中で分岐数が異なるノードが存在してもよいし、また、ルートからリーフへ至るノード数（レベル数）が全てのリーフについて同じである必要はなく、異なるレベルに位置するリーフが存在してもよい。

【００８２】

ここでは、公開鍵及び各ユーザＩＤに対応するユーザシステムの復号鍵の生成処理について説明する。なお、図１４に示すフローチャートには、各ユーザＩＤに対応するユーザシステムの復号鍵の生成処理を示している。

【００８３】

コンテンツ提供システム１は、ユーザ集合Ｕを、共通要素を持たないＬ個以下の部分集合（サブグループ）に分割する（ＳＴ１０１）。簡単のため、サブグループ数をＬとし、Ｌは２のべき乗で表される数とする。コンテンツ提供システム１は、全リーフ数がＬ、木の深さが$D=\log_2 L$である完全二分木を生成し、Ｌ個のサブグループを異なるリーフに割り当てる（ＳＴ１０２）。以下、各サブグループがどのリーフに割り当てられているかの

情報や各ノードＩＤを含めた木構造をＴと表す。Ｔは公開されている。

【００８４】

一方、公開鍵のもととなるパラメータa_0、…、a_{2k-1}、b_0、…、b_{2k-1}をＺｑからランダムに選択する。また、Ｎに属する各要素ｉについて、c_i、λ_iをＺｑからランダムに選択する。ここで、Ｎの定義は式（１）の下に記載されている。

【００８５】

次に、コンテンツ提供システム１は、公開鍵ｅを計算する。公開鍵ｅは、式（１）のようになる。

【数８】

$$e = (g, g^{\lambda_0}, \cdots, g^{\lambda_{2L-3}}, g^{a_0}, \cdots, g^{a_{2k-1}}, g^{c_0}, \cdots, g^{c_{2L-3}}) \quad (1)$$

【００８６】

木構造Ｔにおいて、ルートを除いたノード及びリーフのＩＤの集合をＮとする。簡単のため、全リーフ数がＬである完全二分木におけるＮをＮ＝｛０、…、２Ｌ－３｝とする。図１３の例では、Ｎ＝｛０、…１３｝である。

【００８７】

木構造Ｔのノード・リーフ（ｖ）に、ルート・ノード・リーフでそれぞれ異なる個別鍵生成多項式Ａｖ（ｘ）と、ルート・ノード・リーフで共通の共通鍵生成多項式Ｂ（ｘ）を割り当てる（ＳＴ１０３）。なお、ルート・ノード・リーフで共通の共通鍵生成多項式Ｂ（ｘ）は、あえて、各ルート・ノード・リーフへ割り当てなくてもよい。

【００８８】

さらに、各サブグループに、当該サブグループに割り当てられたリーフ及びその祖先ノードに割り当てられた個別鍵生成多項式を割り当てる（ＳＴ１０４）。

【００８９】

あるノードｖを祖先に持つリーフに割り振られたユーザ集合をU_vとする。図１３では、例えば、$U_8 = U_0 + U_1$である。ここで、＋は和集合を表す。

【００９０】

最後にコンテンツ提供システム１は、ノードｖを祖先ノードにもつリーフに割り振られたユーザ集合（部分集合）U_vに属するユーザＩＤ＝ｕの復号鍵を、鍵生成多項式A_v（ｘ）、Ｂ（ｘ）にｘ＝ｕを代入して算出する（ＳＴ１０５）。ここで、鍵生成多項式A_v（ｘ）、Ｂ（ｘ）は、ユーザｕの属する部分集合U_vに割り当てられ、式（２）のように表される。ここで、λ_vは、ノードｖに割り当てられた、ノードｖ固有の定数値である。

【数９】

$$A_v(x) = \sum_{i=0}^{2k-1} (a_{v,i} - \lambda_v b_i) x^i \bmod q$$

$$B(x) = \sum_{i=0}^{2k-1} b_i x^i \bmod q \quad (2)$$

$$a_{v,i} = \begin{cases} a_i (i \neq v \bmod 2k) \\ c_v (i = v \bmod 2k) \end{cases}$$

【００９１】

例えば、木構造上のあるノードｉを祖先に持つリーフに割り振られたユーザ集合をU_i、当該ノードｉに割り当てられている個別鍵生成多項式をA_i（ｘ）とすると、当該ユー

ザ集合U_iの復号鍵生成多項式は、例えば

$A_i(x)+\lambda_i B(x)=a_0+c_i x+a_2 x^2+\cdots+a_{2k-1}x^{2k-1}$

となる。また、木構造上のノードｊとは異なるノードｉを祖先に持つリーフに割り振られたユーザ集合をU_j、当該ノードｊに割り当てられている個別鍵生成多項式を$A_j(x)$とすると、当該ユーザ集合U_jの復号鍵生成多項式は、例えば

$A_j(x)+\lambda_j B(x)=a_0+c_j x+a_2 x^2+\cdots+a_{2k-1}x^{2k-1}$

となる。

【００９２】

このように、ノードｉを祖先にもつリーフに割り振られたユーザ集合Ｕｉの復号鍵生成多項式、ノードｊを祖先にもつリーフに割り振られたユーザ集合U_jの復号鍵生成多項式は、木構造上のルート・ノード・リーフに固有の１つまたは複数の係数（ここでは、例えば、c_i、c_j）を除き、同じ次数の係数は、ｉ、ｊによらず一定である。

【００９３】

すなわち、ノードｉに割り当てられている個別鍵生成多項式$A_i(x)$と、ルート・ノード・リーフに共通の共通鍵生成多項式Ｂ（ｘ）との同じ次数の係数の線形和のうちの少なくとも１つは、木構造上のルート・ノード・リーフに固有の係数であり、それ以外は、［$A_i(x)$のｍ次係数］＋［$\lambda_i B(x)$のｍ次係数］は、ｉ、ｊによらず一定である。

【００９４】

ノードｉを祖先にもつリーフに割り振られたユーザ集合Ｕｉに属するユーザＩＤ＝ｕの復号鍵は、上記復号鍵生成多項式$A_i(x)+\lambda_i B(x)$の「ｘ」に「ｕ」を代入することにより得られる。

【００９５】

ここで、上記の例では、最大結託人数をｋと設定した場合、安全性の観点から鍵生成多項式の次数を２ｋ－１以上にすることが望ましいため、次数を２ｋ－１としているが、これに限らず、鍵生成多項式の次数として任意の値を設定することが可能である。また、ノードｉに割り当てる鍵生成多項式$A_i(x)$とノードｊに割り当てる鍵生成多項式$A_j(x)$の次数が異なっていても構わないし、鍵生成多項式$A_i(x)$とＢ（ｘ）の次数が異なっていても構わない。これは、後述する他の実施形態でも同様である。

【００９６】

ユーザＩＤ＝ｕのユーザの復号鍵をd_uとすると、d_uは式（３）で表される。

【数１０】

$$d_u=\{(u,v,A_v(u),B(u))\mid v\in N,u\in U_v\} \qquad (3)$$

【００９７】

図１３において、例えば、ユーザｕがリーフ０に割り当てられているとすると、d_uは式（４）で表される。

【数１１】

$$d_u=\{(u,0,A_0(u),B(u)),(u,8,A_8(u),B(u)),(u,12,A_{12}(u),B(u))\} \qquad (4)$$

【００９８】

なお、上記鍵生成フェーズにおける処理は、図１２に示すように、コンテンツ提供システム１以外の信頼できる第三者装置１０ｂが行ってもよい。また、式（４）では、リーフ０のサブグループに、ルートのノード（ノードｖ＝「１４」）に割り当てられた個別鍵生成多項式を割り当てていないが、リーフ０のサブグループに、ルートに割り当てられた個別鍵生成多項式を割り当ててもよい。この場合、ユーザＩＤ＝ｕのユーザの復号鍵を示す式（４）には、当該ルートの鍵生成多項式を用いた復号鍵（ｕ，１４，$A_{14}(u)$，Ｂ（ｕ））が追加される。また、個別鍵生成多項式が割り当てられないノードがあってもよく

、この場合、公開鍵ｅの計算において、対応するc_i、λ_iの生成は不要となる。これらは以下の各実施形態でも同様である。

【００９９】

（暗号化フェーズ）

コンテンツ提供システム１のセッション鍵生成部１３は、ユーザ区分管理部１２からの情報（電子透かし情報がいくつ必要かなど）に基づき、セッション鍵のもととなる情報ｓをＧｑから、ziをＺqからランダムに選択する。電子透かし情報ｉが埋め込まれているコンテンツを得るユーザ識別情報（ユーザシステム）の集合をユーザセグメントχ_iと定義する。

【０１００】

コンテンツ提供システム１の操作者（又は外部の第三者）は、ユーザ集合Ｕを複数のユーザセグメントに分け、ユーザセグメントに関する情報をユーザ区分管理部１２へ入力する。（入力された情報はユーザ区分情報管理部に記憶される。）セッション鍵生成部１３は、ユーザ区分管理部１２からの入力に基づき、各ユーザセグメントに割り当てられる異なる複数のセッション鍵のもととなる情報を生成し、それらの情報をヘッダ生成部１５へ与える。ヘッダ生成部１５は、各ユーザセグメントに異なる複数のセッション鍵をそれぞれ割り当てる。例えば、第１のユーザセグメントχ_1には、セッション鍵s_1を割り当て、第２のユーザセグメントχ_2にはセッション鍵s_2を割り当てる。この割り当ては、セッション鍵生成部１３が行ってもよい。簡単のため、以下の説明では、上記処理の主体者を全てヘッダ生成部１５として記述する。

【０１０１】

次に、ヘッダ生成部１５は、図１６に示すように、ユーザ集合Ｕから複数のユーザセグメントχ_1、χ_2、…χ_jを決定し、以下の２つの条件を満たす、少なくとも１つのリーフＩＤを含めた$\log_2 L+1$個のノードＩＤを選択する。

【０１０２】

なお、以下の説明において、$\log_2 L$をβと表記することもある。

【０１０３】

条件１：選択されるノードをv_0、…、v_βとするとき、和集合$Uv_0+\cdots+Uv_\beta$がユーザ集合Ｕに等しい。

【０１０４】

条件２：式Ｅ１または式Ｅ２を満たす。

【数１２】

$$\chi_i \cap Uv_j = Uv_j \qquad \cdots (E1)$$

いずれのi$(1 \leq i \leq m)$に対しても式(E1)は不成立であり、

$$\text{かつ} \left| Uv_j \setminus Vv_j \right| \leq 2k \qquad \cdots (E2)$$

ここで、

$$Vv_j = \cup_{1 \leq \tau \leq \log_2 L+1, \tau \neq j} Uv_\tau \qquad \cdots (E3)$$

と定義する。

【０１０５】

図１３では、３つのユーザセグメント（ｍ＝３）χ_1、χ_2、χ_3を決定し、４つのノードＩＤ（「０」、「１」、「９」、「１３」）が選択されている。

【０１０６】

次に、ヘッダ生成部１５は、乱数r_0、r_1を選択し、$0 \leqq j \leqq \log_2 L$（＝β）について

、すなわち、選択された各ノードについて（各ノードに属する１又は複数のサブグループからなるグループについて）、以下の処理を繰り返し、選択された各ノードに対し、ヘッダ情報Hv_0、…、Hv_βを計算する（図６のＳＴ２－１～ＳＴ２－８）。

【０１０７】

ヘッダ生成部１５は、集合χ_iとUv_jとの積集合がUv_jであるか否かを判定する（ＳＴ２－４）。

【０１０８】

ここで、χ_iとUv_jとの積集合がUv_jである場合を述べる。これは、Uv_jに属するユーザ全員が、１つの電子透かし情報ｉが埋め込まれたコンテンツを得る場合であり、例えば、図２のU_1が対応する。ヘッダ生成部１５は、次式（５）に従いHv_jを計算する（ＳＴ２－５）。

【数１３】

$$
\begin{aligned}
&H_{v_j} \\
&= (\bar{h}_{v_j}(= g^{r_{v_j}}), \hat{h}_{v_j}(= g^{\lambda_{v_j} r_{v_j}}), h_{v_j,0}, \ldots, h_{v_j,2k-1}), \\
&h_{v_j,t} = \begin{cases} g^{a_t r_{v_j}} & (t \neq v_j \bmod 2k) \\ s_i g^{c_{v_j} r_{v_j}} & (t = v_j \bmod 2k, \chi_i \cup Uv_j = Uv_j) \end{cases} \\
&s_i = s g^{z_i} \qquad \cdots (5)
\end{aligned}
$$

ここで、ｓはG_qから、z_iはZ_qからランダムに選択する。下記処理（式E2を満たすノードに対する処理）が行なわれた場合、$r_{vj} = r_0$とする。そうでない場合、r_{vj}はr_0またはr_1とする。

【０１０９】

例えば、ステップＳＴ２－４及びステップＳＴ２－６の判定のみ先に行ってもよい。ステップＳＴ２－４の結果がそれ以外となる場合（ＳＴ２－４；ＮＯ）が存在しないと判明している場合、ｒにr_0、r_1のどちらを代入してもよい。そうでない場合、ｒにr_0を代入する。

【０１１０】

一方、ステップＳＴ２－４の結果がそれ以外となる場合を述べる（ＳＴ２－４；ＮＯ）。これは、Uv_jに属するユーザの少なくとも１人は集合χ_iに属さず、かつ少なくとも１人は集合χ_iに属する場合であり、例えば、図２のU_2に対応する。

【０１１１】

ヘッダ生成部１５は、ユーザ集合Uv_jに属するユーザＩＤのグループからユーザ集合Vv_jに属するユーザＩＤを取り除いた集合を$Uvj-Vvj=\{\alpha_1, \cdots, \alpha_m\}$とする。

【０１１２】

ここで、Vvjについて説明する。選択された各ノードv_jについて、全てのUv_jがそれぞれ互いに共通要素を持たない場合、定義式（Ｅ３）から、$Uvj-Vvj=Uvj$であるため、ユーザ集合Uv_jに属するユーザＩＤのグループを$\{\alpha_1, \cdots, \alpha_m\}$とすることと等価である。一方、図１３に示したように、U1のうちk人がχ_1に属し、残りのk人がχ_2に属する場合、例えば、ノード０、１、９、１３を選択することができるが、これに代えてノード０、８、９、１３を選択することも可能である。後者の場合、U0とU8は共通要素を持つため、α_1、…、α_mを設定する際には、$Uvj-Vvj=\{\alpha_1, \cdots, \alpha_m\}$とする。例えば、U8－V8=U8－（U0＋U9＋U13）=U1となる。このように、記号Vvjはある二つのUv_jが共通要素を持つ場合を扱うために定義している。

【０１１３】

次に、ヘッダ生成部１５は、２ｋ－ｍ＞０ならば、α_{m+1}、…、α_{2k}をＺｑ－（Ｕ＋｛０｝）からランダムに選択する。なお、Ｚｑ－（Ｕ＋｛０｝）は、ＺｑからＵと｛０｝の和集合を取り除いたものを意味する。

【０１１４】

ヘッダ生成部１５は、１≦ｔ≦２ｋについて、式（８ａ）を満たすＺｑの要素L_0、…、L2k-1を求める。なお、次式（８a）においてαt∈χiに満たす要素αtの数Mが２ｋ未満の場合、式（８ｂ）に示すように、条件式の数が２ｋ（要素Ｌｉの数）となるように式（８a）に条件式を追加してもよいし、式（８ｃ）に示すように、条件式の数を減らしてもよい。また、第２の実施形態において説明するように、条件式の数は２ｋより大きくすることも可能である。

【数１４】

$$\sum_{l=0}^{2k-1} L_l \alpha_t^l = z_i \alpha_t^{v_j \bmod 2k} \bmod q \quad (\alpha_t \in \chi_i) \qquad \cdots (8a)$$

$$\sum_{l=0}^{2k-1} L_l \alpha_t^l = \begin{cases} z_i \alpha_t^{v_j \bmod 2k} \bmod q (\alpha_t \in \chi_i), \\ z'_t \bmod q \qquad (\alpha_t \in Zq \setminus (U \cup \{0\})) \end{cases} \qquad \cdots (8b)$$

$$\sum_{l=0}^{M-1} L_l \alpha_t^l = z_i \alpha_t^{v_j \bmod 2k} \bmod q \quad (\alpha_t \in \chi_i) \qquad \cdots (8c)$$

ここで、z′tは、Ｚｑ上の任意の値である。

【０１１５】

次に、ヘッダ生成部１５は、ｒにｒ１を代入し、式（９）に従いHvjを計算する（ＳＴ２－６）。

【数１５】

$$H_{v_j} = (\bar{h}_{v_j} (= g^{r_{v_j}}), \hat{h}_{v_j} (= g\lambda_{v_j} r_{v_j}), h_{v_j,0}, \ldots, h_{v_j,2k-1}),$$

$$h_{v_j,i} = \begin{cases} g^{L_i} g^{a_i r_{v_j}} & (i \neq vj \bmod 2k) \\ sg^{L_i} g^{c_{v_j} r_{v_j}} & (i = vj \bmod 2k) \end{cases} \qquad \cdots (9)$$

【０１１６】

式（８ａ）（８ｂ）（８ｃ）に示すように、ユーザセグメントχｉに関する値｛L_0，…，L_{2k-1}｝は、これを第１ベクトルとし、当該ユーザセグメントχｉに属するユーザＩＤ（x_w）を２ｋ－１次多項式の変数とし、これを第２ベクトル（１，x_w，x_w^2，…，x_w^{2k-1}）とした場合、当該第１ベクトルと当該第２ベクトルとの内積が、ユーザＩＤに該ユーザＩＤが属するグループ（選択されたノード）のグループ識別情報（ノードＩＤ）v_jに基づく値　v_j mod 2kをべき乗した値に、ユーザセグメント毎に異なる定数ｚｉを乗じた値に等しいという、下記式の関係を満たす第１ベクトルである。

【０１１７】

$(L_0, L_1, L_2, \cdots, L_{2k-1}) \cdot (1, x_w, x_w^2, \cdots, x_w^{2k-1})$
$= z_i x_w^{vj \bmod 2k} \bmod q$

但し、x_wはユーザセグメントχ_iに属するユーザＩＤである。

【０１１８】

なお、上述の例では、m≦２ｋを想定しているが、鍵生成多項式の次数を増やすことにより、m≦（鍵生成多項式の次数＋１）の範囲までmの値を許容できる。

【０１１９】

また、上述の例では、ユーザＩＤに該ユーザＩＤが属するグループ（選択されたノード）のグループ識別情報（ノードＩＤ）v_jに基づく値として$v_j \bmod 2k$を用いているが、これに限らず、v_jを０以上鍵生成多項式の次数以下に一意に写像する関数にv_jを代入した値を用いることができる。

【０１２０】

また、上述の例では、ステップＳＴ２－４の結果がそれ以外となる場合（ＳＴ２－４；ＮＯ）が２回以上発生した場合でも$r = r_1$としているが、これに限らず、ｒに代入される乱数を３つ以上用意し、ステップＳＴ２－４の結果がそれ以外となる場合が発生する度に、ｒに異なる乱数を代入してもよい。また、上述の２つの条件（条件１、２）に加えて、条件２を満たすノードは高々１つ選択されるという条件を導入し、ノードを選択してもよい。この場合、ステップＳＴ２－４の結果がそれ以外となる場合が発生するのは高々１回となる。

【０１２１】

また、上述の例では、ステップＳＴ２－４の結果がそれ以外となる場合（ＳＴ２－４；ＮＯ）に、式（９）に従いHv_jを計算している（ＳＴ２－６）が、これに限らず、χ_iとUv_jとの積集合がUv_jである場合（ＳＴ２－４；ＹＥＳ）であっても、Uv_jの要素数が2k以下（後述する第２の実施形態においては2(d+1)k以下）であれば、式（９）に従いHv_jを計算してもよい。上述のこれらは全て、後述する他の実施形態においても同様である。

【０１２２】

以上の繰り返し処理により得られたHv_0、…、Hv_βをヘッダH（χ）とする（ＳＴ２－９）。ここで、ヘッダは公開鍵ｅを用いて計算できるので、誰でもコンテンツ提供システム１を運営することができる。

【０１２３】

また、以上の繰り返し処理により得られたHv_0、…、Hv_βを構成する各要素の中での同一要素を１つにまとめ、ヘッダH（χ）内にて共有化することにより、送信オーバヘッドをより削減することができる。これは以下の各実施形態でも同様である。

【０１２４】

上述の例では、$\log_2 L + 1$個のノードを選択しているが、これに限らず、選択するノードの数は、これより多くてもよいし、少なくてもよい。すなわち、βを$\log_2 L$以外の値としてもよい。また、上述の例では少なくとも１つのリーフＩＤを選択しているが、上述の２つの条件（条件１，２）が満たされるならば、リーフを選択しなくてもよい。これらは以下の各の実施形態においても同様である。

【０１２５】

上述の例では、コンテンツの復号を禁止されたユーザ（復号鍵を無効化されたユーザ）がいない場合について説明したが、参考許文献２（松下、著作権保護のためのブラックボックス不正者追跡方式に関する研究、東京大学学位論文、２００６年３月）において開示された復号鍵無効化方法を用いることにより、特定のユーザの復号鍵を無効化することも可能である。これは以下の各実施形態でも同様である。

【０１２６】

コンテンツ暗号化部１４は、セッション鍵ｓｉを用いて、電子透かし情報ｉが埋め込まれたコンテンツを暗号化し、ブロードキャストまたはマルチキャストする。

【０１２７】

（復号フェーズ）

ノードｖ$_j$以下のリーフに割り当てられたサブグループからなるユーザ識別情報のグループＵｖ$_j$に属するユーザｕを考える。ユーザＩＤ＝ｕのユーザシステム２は、図８に示すように、ヘッダＨ（χ）を受信した場合（ＳＴ５－１）、Ｈｖ$_j$を用いて式（１０）を計算する。

【数１６】

$$\left(\frac{\prod_{i=0}^{2k-1} h_{v_j,i}^{u^i}}{h_{v_j}^{-A_{vj}(u)} \hat{h}_{v_j}^{B(u)}}\right)^{1/u}{}^{v_j \bmod 2k} = s' \left\{\frac{g^{r_{v_j} \sum_{i=0}^{2k-1} a_{v_j,i} u^i}}{g^{r_{v_j}(A_{v_j}(u)+\lambda_{v_j} B(u))}}\right\}^{1/u}{}^{v_j \bmod 2k} = s' \quad \cdots (10)$$

さらに、上式の右辺は以下のように計算される。

$$s' = \begin{cases} s_i & (\chi_i \cap Uv_j = Uv_j), \\ s\left(g^{\sum_{i=0}^{2k-1} L_i u^i}\right)^{1/u}{}^{v_j \bmod 2k} & (\text{式(E2)が成立する場合}) \end{cases}$$

$$= s_i (u \in \chi_i)$$

【０１２８】

ここで、ヘッダ情報からセッション鍵を復号した結果について簡単に説明する。

ユーザシステム２のセッション鍵復号部２２における復号結果は、ユーザセグメントχｉとＵｖ$_j$の積集合がＵｖ$_j$であるか否かによって場合分けされる（ＳＴ５－４）。なお、ユーザシステム２のセッション鍵復号部２２がこれを判定することはなく、どの場合においても復号手順は共通であり、Ｈｖ$_j$を用いて式（１０）を計算する。

【０１２９】

まず、χｉとＵｖ$_j$の積集合がＵｖ$_j$である場合（ＳＴ５－２；ＹＥＳ）を述べる。これは、Ｕｖ$_j$に属するユーザ全員が同じ電子透かし情報ｉが埋め込まれたコンテンツを得る場合である。例えば、図２のＵ$_1$が対応する。セッション鍵復号部２２は、式（１０）のように計算し（ＳＴ５－５）、該電子透かし情報ｉに対応するセッション鍵ｓｉを得る（ＳＴ－８）。そして、このセッション鍵ｓｉを用いて、Ｕｖ$_j$に属するユーザ全員が、該セッション鍵ｓｉで暗号化されている、電子透かし情報ｉが埋め込まれたコンテンツを得る（ＳＴ－９）。

【０１３０】

次に、χｉとＵｖ$_j$の積集合がＵｖ$_j$である場合（ＳＴ５－４；ＮＯ）を述べる。これは、Ｕｖ$_j$に属するユーザの少なくとも１人はユーザセグメントχ$_i$に属さず、かつ少なくとも１人はユーザセグメントχ$_i$に属する場合であり、例えば、図２のＵ$_2$が対応する。この場合においても、セッション鍵ｓｉは式（１１）が成立することから、セッション鍵復号部２２は、式（１０）のように計算する（ＳＴ５－３）。その結果、各ユーザセグメントχｉに属するユーザシステムでは、該ユーザセグメントχｉに対応するセッション鍵ｓｉを得（ＳＴ８）、このセッション鍵ｓｉを用いて、該セッション鍵ｓｉで暗号化されている、電子透かし情報ｉが埋め込まれているコンテンツを得る（ＳＴ－９）。

【数１７】

$$\sum_{l=0}^{2k-1} L_l u^l = z_i u^{v_j \bmod 2k} \bmod q \qquad \cdots(11)$$

【０１３１】

（追跡フェーズ）

次に、追跡アルゴリズムの手順例を示すが、その前に追跡装置３０とその追跡対象となる不正ユーザについて概略を述べる。追跡装置３０は、海賊版復号器（不正復号器）が押収された場合に、ブラックボックス追跡により、該海賊版復号器の不正作出のもととなった不正ユーザ（のユーザＩＤ）を特定するためのものである。

【０１３２】

正当な復号装置をもとにして海賊版復号器が作出される場合、１台の復号装置のみをもとにして作出される場合と、複数台の復号装置をもとにして作出される場合とがある。後者の場合の復号装置の不正ユーザを結託者と呼ぶ。

【０１３３】

１台の復号装置のみをもとにして作出された海賊版復号器は、当該復号装置と同じ復号鍵が使用可能になる。複数台の復号装置をもとにして作出された海賊版復号器は、当該複数の復号装置と同じ復号鍵がいずれも使用可能になる。後者の場合、結託者に対する全ての復号鍵が無効化されない限り、セッション鍵を得ることが可能になる。

【０１３４】

この追跡装置３０は、複数の不正ユーザが結託した場合に対しても、従来のｎＣｋ通りの検査と比べ、迅速に検査を実行でき、１以上の不正ユーザを特定するものである。

【０１３５】

（手順例）

具体的な追跡アルゴリズムの手順については様々なバリエーションが可能であり、以下に示すものに限定されるものではない。図９は追跡装置による追跡フェーズの動作を説明するためのフローチャートである。

【０１３６】

海賊版復号器Ｄが押収されたとき、以下の処理により不正ユーザを特定する。

【０１３７】

なお、木構造Ｔにおいて、各リーフには２ｋ人のユーザからなるサブグループが割り当てられている。各リーフＩＤを、一番左のリーフから１、…、ｔとし、サブグループU_1、…、U_tの要素（ユーザＩＤ）は、式（１３）のようにラベル付けされているとする。

【数１８】

$$\begin{aligned} U_1 &= \{u_1, \ldots, u_{2k}\}, \\ U_2 &= \{u_{2k+1}, \ldots, u_{4k}\} \\ &\vdots \\ U_t &= \{u_{n-2k+1}, \ldots, u_n\} \end{aligned} \qquad (13)$$

【０１３８】

ここで、各サブグループU_1、…、U_tの要素数（各リーフに属するユーザ数）は全て等しく２ｋでなくてもよい。例えば、サブグループU_1の要素数とサブグループU_2の要素数が異なっていてもよい。これは以下の各実施形態でも同様である。

【０１３９】

追跡装置３０は、ｊ＝１、…、ｎ（ｎ：ユーザ総数、ｊ：ユーザ番号）について以下の処理を実行する（ＳＴ１１～ＳＴ２１）。制御部３３は、電子透かし情報Ａが埋め込まれているコンテンツを得た回数C_j＝０、電子透かし情報Ａが埋め込まれている第１のコンテンツを得るユーザの集合をユーザセグメントχ_Aとする。また、電子透かし情報Ａとは

異なる電子透かし情報Ｂが埋め込まれている第２のコンテンツを得るユーザの集合をユーザセグメントχ_Bとする。同じユーザセグメントχ_A及びユーザセグメントχ_Bに対する検査回数ｚを初期値「１」に設定し、以下の処理をｍ回（検査回数ｚがｍになるまで）繰り返す（ＳＴ１２）。なお、電子透かし情報Ａが埋め込まれている第１のコンテンツをセッション鍵s_Aで暗号化し、電子透かし情報Ｂが埋め込まれている第２のコンテンツをセッション鍵s_Bで暗号化するものとする。

【０１４０】

制御部３３は、ユーザセグメントχ_Bに属するユーザＩＤを$\{u_1、\cdots、u_j\}$とし、それ以外のユーザＩＤをユーザセグメントχ_Bとする（ＳＴ１３）。従って、初期のユーザセグメントχ_Bに属するユーザＩＤは$\{u_1\}$、初期のユーザセグメントχ_Aに属するユーザＩＤは$\{u_2、\cdots、u_n\}$となる。また、制御部３３は、ヘッダ生成部３２を制御し、暗号化されるセッション鍵の数を「２」として、つまりs_Aとs_Bをセッション鍵として、ヘッダＨ（χ）を生成させる（ＳＴ１４）。なお、ヘッダ生成方法は暗号化フェーズに示した方法と同様であり、乱数は毎回ランダムに選択される。

【０１４１】

ヘッダ生成部３２が、ヘッダＨ（χ）と、暗号化コンテンツ（s_Aを用いて透かし情報Ａが埋め込まれている第１のコンテンツを暗号化したものと、s_Bを用いて透かし情報Ｂが埋め込まれている第２のコンテンツを暗号化したもの）を不正復号器Ｄに入力すると（ＳＴ１５）、制御部３３は、不正復号器Ｄの出力を観察する。

【０１４２】

このとき、制御部３３は、不正復号器Ｄが第１のコンテンツを出力したのか、第２のコンテンツを出力したのか検出し（ＳＴ１６）、第１のコンテンツを出力した場合（ＳＴ１６；ＹＥＳ）、C_jを「１」だけインクリメントする（ＳＴ１７）。第２のコンテンツを出力した場合（ＳＴ１６；ＮＯ）、C_jの値を変化させない。

【０１４３】

なお、セッション鍵自体がコンテンツである場合、つまりセッション鍵s_Aに電子透かし情報Ａが埋め込まれ、セッション鍵s_Bに電子透かし情報Ｂが埋め込まれている場合、ヘッダのみを不正復号器Ｄに入力し、電子透かし情報Ａが埋め込まれているコンテンツが復号されていればC_jを「１」だけインクリメントし、そうでなければC_jの値は変化しないようにすればよい。

【０１４４】

いずれにしても、制御部３３は、C_jの更新が終わると、検査回数ｚがｍ回未満か否かを判定し（ＳＴ１８）、ｍ回未満であればｚを「１」だけインクリメントし（ＳＴ１９）、ステップＳＴ１４に戻って検査を繰り返す。

【０１４５】

また、制御部３３は、ステップＳＴ１８の判定の結果、検査回数ｚがｍに等しくなると、ユーザセグメントχ_Bに属するユーザ番号ｊがユーザ総数ｎ未満か否かを判定し（ＳＴ２０）、ｎ未満であればｊを「１」だけインクリメントし（ＳＴ２１）、ステップＳＴ１２に戻って検査を繰り返す。

【０１４６】

ステップＳＴ２０の判定の結果、ユーザセグメントχ_Bに属するユーザu_jのユーザ番号ｊがユーザ総数ｎに一致すると検査が終了する。

【０１４７】

次に、制御部３３は、ｊ＝１、…、ｎについて、得られた$C_{j-1}-C_j$を計算し、$C_{j-1}-C_j$が最大値となる整数ｊを検出すると（ＳＴ２２）、u_jを不正ユーザと特定してそのユーザＩＤを出力する（ＳＴ２３）。

【０１４８】

この追跡方法では、図１０及び図１１に示すように、ユーザセグメントχ_Bに属する不正ユーザの候補を一人ずつ増やし、不正ユーザの候補をユーザセグメントχ_Bに含めたときに電子透かし情報Ｂが埋め込まれている第２のコンテンツを出力するか（言い換えれば

、透かし情報Ａが埋め込まれている第２のコンテンツを出力しないか）を検査しており、この検査を合計ｍｎ回行うことにより、１人以上の不正ユーザを特定することができる。なお、ｍｎ回の検査は、上述したような順番以外に、ランダムな順番で行ってもよい。これは、以下の実施例においても同様である。

【０１４９】

例えば、ユーザＩＤの集合を｛u_1、…、u_n｝とし、検査対象復号装置２０χの結託者のユーザＩＤ＝u_2、u_4であるとする。

【０１５０】

この場合、ユーザＩＤ＝u_1、u_2、u_3をユーザセグメントχ_B、残りのユーザＩＤをユーザセグメントχ_Aとして生成したヘッダ情報を与えると、該検査対象復号装置２０χはユーザＩＤ＝u_4に対応しているので、セッション鍵s_Aが得られて、電子透かし情報Ａが埋め込まれている第１のコンテンツが出力される。従って、ｍ回の繰り返し処理後C_3＝ｍとなる。

【０１５１】

また、ユーザＩＤ＝u_1、u_2、u_3、u_4をユーザセグメントχ_B、残りのユーザＩＤをユーザセグメントχ_Aとして生成したヘッダ情報を与えると、該検査対象復号装置からは、セッション鍵s_Aが得られず、替わりにセッション鍵s_Bが得られるので、電子透かし情報Ｂが埋め込まれている第２のコンテンツが出力される。従って、ｍ回の繰り返し処理後C_4＝０となる。

【０１５２】

したがって、$C_3 - C_4$が最大値ｍを与えるため、該検査対象復号装置２０χの結託者のうちの１人のユーザＩＤは、u_4であることがわかる。さらに、ユーザのラベル付けの順序を変えることにより、結託者全員のユーザＩＤを特定することも可能である。

【０１５３】

より一般的には、$C_{j-1} - C_j \geqq m/n$となる整数ｊが少なくとも１つは存在し、ユーザＩＤ＝u_iのユーザが不正ユーザでないとき$C_{i-1} - C_i << m/n$であることから、$C_{j-1} - C_j$が最大値となる整数jを検出することにより不正ユーザＩＤを特定できる。

【０１５４】

電子透かし情報Ａ及びＢがそれぞれ埋め込まれている第１及び第２のコンテンツは、ともに正常なコンテンツであるため、検査対象復号装置は、過去の入力を記憶していたとしてもブラックボックス追跡を検知することができず、必ず電子透かし情報Ａ、Ｂのうちのいずれかが埋め込まれているコンテンツを出力する。従って、上述の方法により確実に不正ユーザの特定できる。

【０１５５】

ここで、ヘッダは公開鍵ｅを用いて計算できるので、誰でも追跡装置３０を用いて不正ユーザを追跡することができる。

【０１５６】

上述の例では、容疑者を一人ずつ検査しているが、これに限らず、以下に説明するように２分岐探索を行ってもよい。始めに、ユーザ集合を２分割し、一方の第１の部分集合をユーザセグメントχ_Aとし、他方の第２の部分集合をユーザセグメントχ_Bとして、ヘッダ情報及び暗号化コンテンツを生成し、検査対象復号装置に入力する。検査対象復号装置の出力が電子透かし情報Ａが埋め込まれているコンテンツであった場合、ユーザセグメントχ_Aを２分割し、得られた２つの部分集合のうちのいずれか一方をユーザセグメントχ_Aから取り除き、ユーザセグメントχ_Bへ加える。一方、検査対象復号装置の出力が電子透かし情報Ｂが埋め込まれているコンテンツであった場合、ユーザセグメントχ_Bを２分割し、得られた２つの部分集合のうちのいずれか一方をユーザセグメントχ_Bから取り除き、ユーザセグメントχ_Aへ加える。新たに設定されたユーザセグメントχ_A、χ_Bに対して、上記検査を行う。この処理を容疑者が１人になるまで繰り返す。最後に、ユーザセグメントχ_A（またはユーザセグメントχ_B）に属するユーザが１人に絞り込まれ、検査対象復号装置が電子透かし情報Ａ（または電子透かし情報Ｂ）が埋め込まれているコンテンツを出

力した場合、その１人のユーザを不正ユーザと特定する。

【０１５７】

また、用意するセッション鍵の数（埋め込む透かし情報の数）Ｊを３以上にして、Ｊ分岐探索を行うことも可能である。これは、以下の実施例においても同様である。

【０１５８】

以上説明したように、複数のユーザシステムへ、暗号化コンテンツと当該暗号化コンテンツを復号するためのヘッダ情報とを提供するコンテンツ提供システムでは、コンテンツ暗号化部１４が、複数のユーザシステムを個別に識別するための複数のユーザ識別情報のグループに割り当てられた異なる複数のセッション鍵s_j（ｊ＝１，２，…、ｎ）を用いてコンテンツを暗号化し、複数の暗号化コンテンツを得る、ヘッダ生成部１５が、複数のセッション鍵のそれぞれを、各ユーザシステム固有の復号鍵に対応する公開鍵で暗号化し、複数の暗号化セッション鍵を得る。さらにヘッダ生成部１５は、該グループに対し、（ａ）上記複数の暗号化セッション鍵と、（ｂ）該グループ内の任意のユーザ識別情報ｕに割り当てられているセッション鍵に対応する第１のベクトル（L_0，L_1，L_2，…，L_{2k-1}）と、該ユーザ識別情報ｕに関する第２のベクトル（１，ｕ，u^2，…，u^{2k-1}）との内積が、$z_j\ u^{v \bmod 2K}$（ここで、z_jは上記複数のセッション鍵に対応する異なる複数の定数値のうち該ユーザ識別情報ｕに割り当てられているセッション鍵s_jに対応する定数値、ｖはグループ識別情報、Ｋは予め定められた正の整数値）に等しくなるように設定された該第１のベクトルと、を含むヘッダ情報を生成する。そして、上記複数の暗号化コンテンツのうちの少なくとも１つ及び上記ヘッダ情報を複数のユーザシステムへ送信する。

【０１５９】

ヘッダ情報には、正しいセッション鍵が複数含まれており、ユーザシステムはこれらの正しいセッション鍵のうちいずれかを常に得るので、ブラックボックス追跡の際に、入力の意図を不正復号器に知られることが無く、過去の入力を記憶し、それを利用して入力の意図を読み取って不正ユーザの特定を阻止しようと動作する巧妙な不正復号器に対しても、確実に追跡を実行することができる。さらに、ユーザ集合を木構造化し、構成された木構造に基づいた鍵生成多項式を導入することにより、同様のブラックボックス追跡が可能な従来方法に比べて、送信オーバヘッドの削減が可能となる。また、不正ユーザなどの特定のユーザを一時的に無効化し、構成された木構造を変更することなく、鍵生成多項式を更新することにより、不正ユーザなどの特定のユーザのみをシステムから排除し、その他のユーザの復号鍵を更新することが可能となる。

【０１６０】

また、上記実施形態によれば、ヘッダ情報は、複数の暗号化セッション鍵を含み、それらを用いて異なる電子透かし情報が埋め込まれた複数のコンテンツをそれぞれ暗号化し、埋め込まれている電子透かし情報を検査することでブラックボックス追跡を行うため、ブラックボックス追跡の際のヘッダ情報（及び暗号化コンテンツ）と通常放送のヘッダ情報（及び暗号化コンテンツ）とは識別不可能である。これにより、ブラックボックス追跡の際に、たとえ不正復号器が過去の入力を記憶していたとしても、各入力の意図が不正復号器に知られることがないため、入力の意図を読み取って不正ユーザの特定を阻止しようと動作する巧妙な不正復号器に対しても、確実に追跡を実行することができる。

【０１６１】

同等の追跡性能を有する従来のブラックボックス追跡方法では、第１のタイプ（方式が組み合わせ論的な構成に基づいている）であるため、送信オーバヘッドを非常に大きくしなければならないという問題があったが、本実施形態では、ユーザ集合を木構造化し、各ノードに鍵生成多項式を割り当て、代数的な構成に基づいてヘッダを生成するため、送信オーバヘッドの削減が可能となる。

【０１６２】

上記実施形態によれば、ブラックボックス追跡の際に、入力の意図を不正復号器に知られることが無く、さらに過去の入力を記憶し、それに基づいて不正ユーザの特定を妨げる

ように動作する巧妙な不正復号器に対しても、確実に追跡を実行でき、しかも、送信オーバヘッドの削減が可能となる。また、不正ユーザが特定された後、不正ユーザをシステムから排除できる。

【０１６３】

（第２の実施形態）

次に、第２の実施形態について説明する。第２の実施形態は、第１の実施形態の暗号化フェーズにおいて、図６のステップＳＴ２－４において、Uv_jに属するユーザの少なくとも１人は集合χ_iに属さず、かつ少なくとも１人は集合χ_iに属す場合（ＳＴ２－４；ＮＯ）、鍵生成多項式の次数を増やすことなく、$m \leqq 2k$となる制限をなくす方法について説明する。第１の実施形態との違いは、ステップＳＴ２－４においてUv_jに属するユーザの少なくとも１人は集合χ_iに属さず、かつ少なくとも１人は集合χ_iに属す場合の暗号化方法とその復号方法のみであるため、それらのみを説明する。

【０１６４】

ｑを素数とし、ｑはｐ－１を割り切り、かつ、ｑはｎ＋２ｋ以上であるとする。

【０１６５】

（暗号化フェーズ）

ステップＳＴ２－４において、Uv_jに属するユーザの少なくとも１人は集合χ_iに属さず、かつ少なくとも１人は集合χ_iに属す場合（ＳＴ２－４；ＮＯ）について述べる。

【０１６６】

ヘッダ生成部１５は、図７に示すように、Uv_jから、集合Vvjを取り除いた部分集合を$\{x_1, \cdots, x_m\}$とする。ここで、ｍは、前述同様、Uv_jに属するユーザ集合のうち、集合Vvjに属さないユーザの総数である。

【０１６７】

次に、ヘッダ生成部１５は、$2dk+1 \leqq m \leqq 2(d+1)k$を満たす整数ｄを探し、$2(d+1)k-m>0$ならば、$x_{m+1}, \cdots, x_{2(d+1)k}$を$Z_q-(U+\{0\})$からランダムに選択する。なお、$Z_q-(U+\{0\})$は、$Z_q$からＵと｛０｝の和集合を取り除いたものを意味する。

【０１６８】

ヘッダ生成部１５は、$1 \leqq t \leqq 2(d+1)k$について、式（１４）を満たすZ_qの要素$L_0, \cdots, L_{2(d+1)k-1}$を求める。

【数１９】

$$\sum_{l=0}^{2(d+1)k-1} L_l x_t^l = \begin{cases} z_i x_t^{y_{v_j}(\sum_{t=0}^{d} 2kt+2)} \bmod q & (x_t \in \chi_i), \\ z_t' \bmod q & (x_t \in Z_q \setminus (U \cup \{0\})) \end{cases}$$

$$y_{v_j} = v_j \bmod 2k \qquad \cdots(14)$$

ここで、z_t'はZ_q上の任意の値である。

【０１６９】

次に、ヘッダ生成部１５は、ｒにr_1を代入し、式（１５）に従いHv_jを計算する（ＳＴ２－６）。

【数２０】

$$H_{v_j} = (\bar{h}_{v_j}(= g^{r_{v_j}}), \hat{h}_{v_j}(= g^{\lambda_{v_j} r_{v_j}}), h_{v_j,0}, \cdots, h_{v_j,2(d+1)k-1}),$$

$$h_{v_j,i} = \begin{cases} g^{L_i} g^{a_i r_{v_j}} & (y_{v_j} \neq i \bmod 2k), \\ s g^{L_i} g^{c_{v_j} r_{v_j}} & (y_{v_j} = i \bmod 2k) \end{cases} \quad \cdots (15)$$

【０１７０】

なお、前述の通り、ｒに代入される乱数を３つ以上用意し、ステップＳＴ２－４の結果がそれ以外となる場合が発生する度に、ｒに異なる乱数を代入することも可能である。

【０１７１】

（復号フェーズ）

部分集合Uv_jに属するユーザｕを考える。図８のＳＴ５－６の場合、Hv_jを用いて式（１６）を計算する。

【数２１】

$$\left(\frac{\prod_{i=0}^{2(d+1)k-1} h_{v_j,i}^{u^i}}{\left(\bar{h}_{v_j}^{-A_{v_j}(u)} \hat{h}_{v_j}^{B(u)} \right)^{\sum_{t=0}^{d} u^{2kt}}} \right)^{1/u^{y_{v_j}(\sum_{t=0}^{d} 2kt+1)}}$$

$$= \left\{ \frac{s^{u^{y_{v_j}(\sum_{t=0}^{d} 2kt+1)}} g^{\sum_{i=0}^{2(d+1)k-1} L_i u^i} \left(g^{r_{v_j} \sum_{i=0}^{2k-1} a_{v_j,i} u^i} \right)^{\sum_{t=0}^{d} u^{2kt}}}{g^{r_{v_j}(A_{v_j}(u) + \lambda_{v_j} B(u)) \sum_{t=0}^{d} u^{2kt}}} \right\}^{1/u^{y_{v_j}(\sum_{t=0}^{d} 2kt+1)}}$$

$$= s \left(g^{\sum_{i=0}^{2(d+1)k-1} L_i u^i} \right)^{1/u^{y_{v_j}(\sum_{t=0}^{d} 2kt+1)}}$$

$$= s g^{z_i} (u \in \chi_i)$$

$$= s_i \quad \cdots (16)$$

【０１７２】

ユーザｕが集合χ_iに属す場合、式（１４）より、セッション鍵ｓｉを得る（ＳＴ８）

上述したように第２の実施形態によれば、ｍ≦２ｋとなる制限をなくす構成により、すなわち、Uv_jに属するユーザの少なくとも１人は集合χ_iに属さず、かつ少なくとも１人は集合χ_iに属す場合に、集合Uvj-Vvjに属するユーザの数を第１の実施形態の場合と比較すると、２ｄｋだけ増やすことができる（式（１４）のx_tの次数が式（８）の「２ｋ－１」から「２(ｄ+1)ｋ－１」に増え、その結果、式（１５）に示すようにヘッダ情報Hv_jの要素の数が、式（９）の「２ｋ＋２」から「２(ｄ+1)ｋ＋２」に増えている）。

【０１７３】

第１の実施形態の効果に加え、ステップＳＴ２－４の結果がそれ以外となる場合（ＳＴ２－４；ＮＯ）において、集合Uvj-Vvjに属するユーザ数が第１の実施形態の説明において述べた制限を超えた場合にも対応できる。また、ｍ≦２ｋとなる制限をなくす構成とし

ても、第１の実施形態と同様の効果を得ることができる。

【０１７４】

（第３の実施形態）

次に、第３の実施形態について説明する。第３の実施形態は、第１、第２の実施形態において、復号鍵の更新を行う例である。第３の実施形態に係る復号鍵更新方法は、全ユーザシステムに対し、それぞれの復号鍵を更新する場合や、例えば、追跡装置３０により不正ユーザのユーザＩＤを特定した場合に、該ユーザＩＤを持つ不正ユーザシステムでのコンテンツ復号を不可能にするために、該不正ユーザシステム以外の正当なユーザシステムに対し、復号鍵を更新する場合などにも用いられる。

【０１７５】

なお、特に断りのない限り、記号は、第１の実施形態において定義されたものを用いる。

【０１７６】

ここで、鍵更新手順の概略を簡単に説明する。前述したように、ノードｖを祖先にもつリーフあるいはリーフｖに割り振られたユーザ集合Ｕｖに属するユーザＩＤ＝ｕの復号鍵は、式（２）に示したような鍵生成多項式A_v（ｘ）、Ｂ（ｘ）を用いて、復号鍵生成多項式A_v（ｘ）＋λ_vＢ（ｘ）の「ｘ」に「ｕ」を代入することにより得られる。そこで、式（２）の鍵生成多項式A_v（ｘ）、Ｂ（ｘ）の係数群$a_{v,i}$、λ_v、b_iを、$a_{v,i}+a'_{v,i}$、$\lambda_v+\lambda'_v$、$b_i+b'_i$と更新することにより（鍵生成多項式自体を更新することにより）、各ユーザシステムの復号鍵を更新する。

【０１７７】

例えば、復号鍵を更新する必要のあるユーザＩＤの集合（ユーザセグメント）に対しては、上記係数群を更新するために必要な情報$a'_{v,i}$、λ'_v、b'_iを含む鍵更新情報をコンテンツとし、これを該ユーザセグメントに割り当てられたセッション鍵で暗号化し、暗号化鍵更新情報を生成する。そして、前述のコンテンツ提供装置がヘッダ情報及び暗号化コンテンツを生成する手法と同様に、暗号化鍵更新情報と、該暗号化鍵更新情報を復号するためのヘッダ情報を生成し、送信する。

【０１７８】

復号鍵を更新する必要のないユーザＩＤの集合（ユーザセグメント）に対しては、該ユーザセグメントに割り当てられたセッション鍵で暗号化された上記鍵更新情報を送信しない。

【０１７９】

この結果、前者のユーザセグメントに属するユーザＩＤのユーザシステムでは、上記鍵更新情報を取得することができ、復号鍵を更新することができるものの、後者のユーザセグメントに属するユーザＩＤのユーザシステムでは、上記鍵更新情報を取得することはできず、復号鍵の更新は行えない。

【０１８０】

以下、図１７に示すフローチャートを参照して、コンテンツ提供システムにおける処理と、ユーザシステムにおける処理をより詳細に説明する。

【０１８１】

コンテンツ提供システムの処理動作は、セッション鍵でコンテンツを暗号化する代わりに、セッション鍵で鍵更新情報を暗号化する以外は、ほぼ図５と同様である。

【０１８２】

図１７において、コンテンツ提供システムは、鍵更新処理を開始する旨の鍵更新開始情報をユーザシステムに送信する（ＳＴ２０１）。ここで、コンテンツ提供システムからユーザシステムへの送信について、１対１の送信でもよいし、複数のユーザシステムへブロードキャスト又はマルチキャストでもよい。これは以下についても同様である。

【０１８３】

コンテンツ提供システムは、Ｌ個（ｊ＝１、２、…Ｌ）の乱数ｓｊ＝s_1、…、s_LをＧｑからランダムに選択する。Ｌ個の乱数は、Ｌ個のリーフにそれぞれ対応する。さらに、

乱数s_1、…、s_Lを公開鍵格納部１１に記憶されている公開鍵で暗号化し、 各リーフvjについて、式（５）によりHV_jを計算する（ＳＴ２０２）。なお、ステップＳＴ２０２におけるヘッダ生成部１５のヘッダ情報の生成処理は、以下の２点を除き、第１の実施形態と同様である（図６等参照）。

【０１８４】

（１）選択するノードは、Ｌ個のリーフである。（２）各リーフvjについて、式（５）によりHV_jを計算する。

【０１８５】

ただし、

【数２２】

$$h_{v_j,t} = \begin{cases} g^{a_t r_{v_j}} & (t \neq v_j \bmod 2k) \\ s_j g^{c_{v_j} r_{v_j}} & (t = v_j \bmod 2k) \end{cases} \quad \cdots(17)$$

但し、 t=0,…,2k-1

【０１８６】

コンテンツ提供システムは、乱数a'_0、…、a'_{2k-1}、b'_0、…、b'_{2k-1}、c'_0、…、c'_{2L-3}、λ'_0、…、λ'_{2L-3}をＺｑからランダムに選択し、１≦ｊ≦Ｌについて、以下の処理を繰り返す。コンテンツ提供システムは、鍵更新情報Mv_jを生成し、該リーフvjに対応する乱数、すなわち、セッション鍵s_jを用いて鍵更新情報Mv_jを共通鍵暗号化する（ＳＴ２０３）。暗号化された鍵更新情報を$M'v_j$と表す。鍵更新情報Mv_jには、リーフv_jの鍵生成多項式A_v（ｘ）、Ｂ（ｘ）の係数群を更新するための情報、すなわち、上記選択された乱数a'_0、…、a'_{2k-1}、b'_0、…、b'_{2k-1}、c'_0、…、c'_{2L-3}、λ'_0、…、λ'_{2L-3}が含まれている。

【０１８７】

ここで、鍵更新情報Mv_jについて説明する。リーフv_jを$v_{j,1}$と書き換え、リーフ$v_{j,1}$からルートに至るまでの各ノードを$v_{j,2}$、…、$v_{j,\log_2 L}$とすると、鍵更新情報Mv_jは次式により表される。

【数２３】

$$M_{v_j} = M_{v_{j,1}} \| \cdots \| M_{v_{j,\log_2 L}} \| b'_0 \| \cdots \| b'_{2k-1}$$

$$M_{v_{j,i}} = a''_{v_{j,i},0} \| \cdots \| a''_{v_{j,i},2k-1}$$

$$a''_{v_{j,i},t} = a'_{v_{j,i},t} - \{(\lambda_{v_{j,i}} + \lambda'_{v_{j,i}})(b_t + b'_t) - \lambda_{v_{j,i}} b_t\} \bmod q$$

$$a'_{v_{j,i},t} = \begin{cases} a'_t & (t \neq v_{j,i} \bmod 2k), \\ c'_{v_{j,i}} & (t = v_{j,i} \bmod 2k) \end{cases} \quad \cdots(18)$$

ここで、||はデータ連結を表す。

【０１８８】

以上の繰り返し処理により得られた$M'v_1$、…、$M'v_L$を暗号化鍵更新情報Ｍ’とする。コンテンツ提供システムは、暗号化鍵更新情報Ｍ’をユーザシステムに送信する（ＳＴ２０４）。なお、送信先であるユーザシステムがUv_jに属することがわかっている場合、Ｍ’vjのみを送信してもよい。

【０１８９】

また、コンテンツ提供システムは、ヘッダ情報Ｈをユーザシステムに送信する（ＳＴ２０４）。ここで、送信先であるユーザシステムがUv_jに属することがわかっている場合、Hv_jのみを送信してもよい。

【０１９０】

コンテンツ提供システムは、次式により新しい公開鍵ｅnewを計算する（ＳＴ２０５）。

【数２４】

$$e_{new} = (g, g^{\lambda_0+\lambda'_0}, \ldots, g^{\lambda_{2L-3}+\lambda'_{2L-3}}, g^{a_0+a'_0}, \ldots, g^{a_{2k-1}+a'_{2k-1}},$$

$$g^{c_0+c'_0}, \ldots, g^{c_{2L-3}+c'_{2L-3}} \quad \cdots(19)$$

【０１９１】

次に、ユーザＩＤがｕであり、そのユーザＩＤがUv_j（v_jはリーフ）に割り当てられたサブグループに属するユーザシステムにおける処理を説明する。ユーザシステムは、鍵更新開始情報を受信すると（ＳＴ２０６）、コンテンツ提供システムにより送られてきたヘッダ情報Ｈ（又はHv_j）を復号し、s_jを取得する（ＳＴ２０７）。ここで、ヘッダ情報Ｈの復号方法は第１の実施形態において説明した復号方法と同様である。

【０１９２】

ユーザシステムは、コンテンツ提供システムにより送られてきた暗号化鍵更新情報Ｍ’より当該ユーザシステムが復号可能なＭ’v_jを選択し（又はＭ’v_jのみを受信し）、ｓｊを用いて Ｍ’v_jを復号し、Mv_jを取得する（ＳＴ２０８）。

【０１９３】

リーフv_jを$v_{j,1}$と書き換え、リーフ$v_{j,1}$からルートに至るまでの各ノードを$v_{j,2}$、…、$v_{j,\log_2 L}$とする。１≦ｉ≦log2 Lについて、ユーザシステムは、次式により新しい復号鍵Ａnew、Ｂnewを計算する（ＳＴ２０９）。

【数２５】

$$A_{new,v_{j,i}}(u) = A_{v_{j,i}}(u) + \sum_{t=0}^{2k-1} a''_{v_{j,i},t} u^t \bmod q,$$

$$B_{new}(u) = B(u) + \sum_{t=0}^{2k-1} b'_t u^t \bmod q \quad \cdots(20)$$

【０１９４】

ここで、鍵生成多項式の各係数は次式に表されるように更新される。

【数２６】

$$A_{new,v}(x) = \sum_{i=0}^{2k-1} \{(a_{v,i} + a'_{v,i}) - (\lambda_v + \lambda'_v)(b_i + b'_i)\} x^i \bmod q,$$

$$B_{new}(x) = \sum_{i=0}^{2k-1} (b_i + b'_i) x^i \bmod q,$$

$$a'_{v,i} = \begin{cases} a'_i & (i \neq v \bmod 2k) \\ c'_v & (i = v \bmod 2k) \end{cases} \quad \cdots(21)$$

【０１９５】

式（１９）と式（２１）から、更新された公開鍵とユーザ復号鍵が対応付けられていることがわかる。

【０１９６】
上述の例では、係数群$a_{v,i}$、λ_V、及びb_iを更新しているが、λ_Vを更新せず（$\lambda'_V=0$と設定し）、$a_{v,i}$及びb_iのみを更新することも可能である。また、λ_V及びb_iを更新せず（$\lambda'_V=0$かつ$b_i'=0$と設定し）、$a_{v,i}$のみを更新することも可能である。この場合、式（１８）において、鍵更新情報Mv_jにb_i'を含めることが不要となる。
【０１９７】
上述の例では、コンテンツ提供システムが、鍵更新開始情報をユーザシステムに送信することにより鍵更新処理を始めているが、ユーザシステムの方から鍵更新を要求する旨の情報をコンテンツ提供システムに送信して鍵更新処理を始めてもよい。また、コンテンツ提供システムは、ヘッダ情報、暗号化鍵更新情報、及び新しい公開鍵を、上述の順序に限らず、どの順序で生成してもよいし、鍵更新開始情報をユーザシステムに送信する前に、ヘッダ情報、暗号化鍵更新情報、及び新しい公開鍵を予め生成しておいてもよい。
【０１９８】
また、参考文献２（松下、著作権保護のためのブラックボックス不正者追跡方式に関する研究、東京大学学位論文、２００６年３月）において開示された復号鍵無効化方法を用いることにより、特定のユーザシステムの鍵更新を行わせないようにし、当該特定のユーザシステムをデータ通信システムから排除することも可能である。
【０１９９】
より具体的には、コンテンツ提供システムは、上述のヘッダ情報Ｈに加え、ｓをＧｑからランダムに選択し、参考文献２において開示された暗号化方法を用いてｓを暗号化し、ヘッダ情報Ｈ’を生成し、ユーザシステムへ送信する。ヘッダ情報Ｈ’においては、ｓの復号を許可されたユーザシステムのみがｓを取得でき、ｓの復号を禁止されたユーザシステム（無効化対象のユーザシステム）はｓを取得できない。コンテンツ提供システムは、鍵更新情報Mv_jを生成し、ある関数Ｆについて、$s'_j=F(s_j,s)$を用いて鍵更新情報Mv_jを共通鍵暗号化する。関数Ｆの例として、例えば、
【数２７】

$$F(s_j,s)=s_j\oplus s$$

⊕はビット毎の排他的論理和を表す。

【０２００】
が挙げられる。
【０２０１】
ユーザシステムは、ヘッダ情報Ｈ及びＨ’を復号し、s_j及びｓをそれぞれ取得する。ユーザシステムは、s'_jを用いて暗号化鍵更新情報を復号し、復号鍵を更新する。このようにすることで、無効化対象のユーザシステムはｓを取得できず、従って復号鍵を更新することができない。
【０２０２】
また、上述の例は、コンテンツ提供システムとユーザシステムとの間において鍵更新処理が行われる例であるが、コンテンツ提供システムの代わりに信頼できる第三者がユーザシステムとの間で鍵更新を行い、更新された公開鍵をコンテンツ提供システムに通知してもよい。
【０２０３】
なお、上記全ての実施形態では、主に「システム」のカテゴリーで表現したが、これに限らず、「装置」、「方法」、「コンピュータ読取り可能な記憶媒体」又は「プログラム」等といった任意のカテゴリーで表現してもよいことは言うまでもない。また、システム全体のカテゴリーを変える場合に限らず、システムの一部を抽出して他のカテゴリーで表現してもよいことも言うまでもない。
【０２０４】
また、上記全ての実施形態の暗号化装置、復号装置、追跡装置は、いずれも、半導体集

積装置などのハードウェアとしても、ソフトウェア（（コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラム）としても、実現可能である。もちろん、ハードウェアとソフトウェアとを併用して実現することも可能である。

【０２０５】

また、プログラムとして実現する場合、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０２０６】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【０２０７】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行してもよい。

【０２０８】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０２０９】

また、記憶媒体は１つに限らず、複数の媒体から上記実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であってもよい。

【０２１０】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【０２１１】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０２１２】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【０２１３】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種

々変形して実施することができる。例えば本願発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

【図面の簡単な説明】

【０２１４】

【図１】本発明の第１の実施形態に係るコンテンツ提供システム及びユーザシステム等が適用されたデータ通信システムの構成を示す模式図である。

【図２】ユーザ集合のサブグループを説明するための模式図である。

【図３】ユーザ集合のサブグループを説明するための模式図である。

【図４】追跡システムの構成を示す模式図である。

【図５】データ通信システムの全体の動作を説明するためのフローチャートである。

【図６】暗号化フェーズの動作を説明するためのフローチャートである。

【図７】ヘッダ生成部の処理を説明するための模式図である。

【図８】復号フェーズの動作を説明するためのフローチャートである。

【図９】追跡フェーズの動作を説明するためのフローチャートである。

【図１０】検査の概要を説明するための模式図である。

【図１１】検査の結果を説明するための模式図である。

【図１２】データ通信システムの変形例を示す模式図である。

【図１３】木構造を説明するための図。

【図１４】復号鍵生成処理動作を説明するためのフローチャート。

【図１５】コンテンツに電子透かし情報の埋め込む方法を説明するための図。

【図１６】ユーザ集合内の複数のユーザセグメントを説明するための図。

【図１７】復号鍵の更新処理を説明するためのフローチャート。

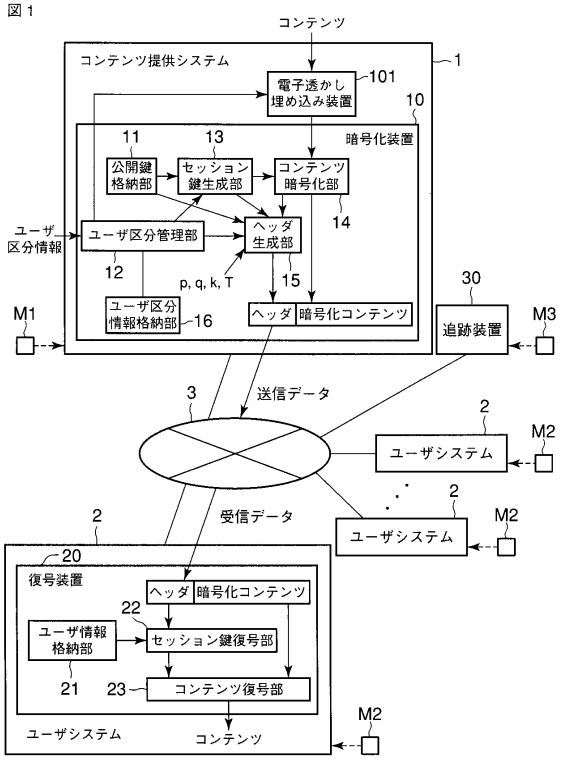
【符号の説明】

【０２１５】

１…コンテンツ提供システム、２…ユーザシステム、３…ネットワーク、１０…暗号化装置、１１，３１…公開鍵格納部、１２…無効化対象ユーザ情報格納部、１３…セッション鍵生成部、１４…コンテンツ暗号化部、１５，３２…ヘッダ生成部、２０…復号装置、２１…ユーザ情報格納部、２２…セッション鍵復号部、２３…コンテンツ復号部、３０…追跡装置、３３…制御部。

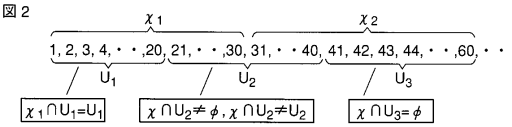
【図１】

図１



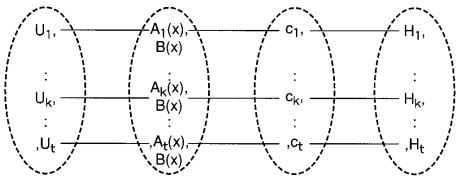
【図２】

図２



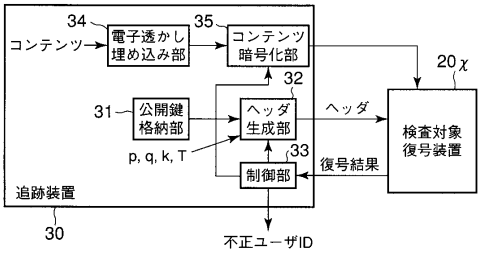
【図３】

図３



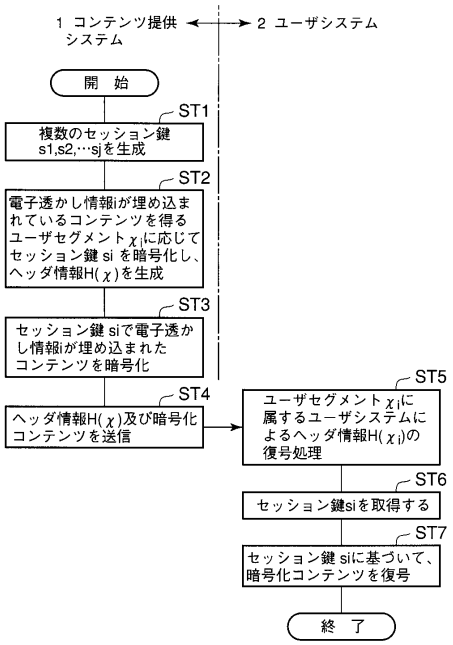
【図４】

図４



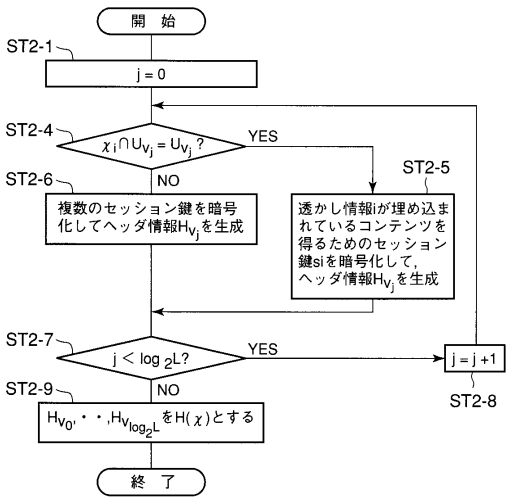
【図５】

図５



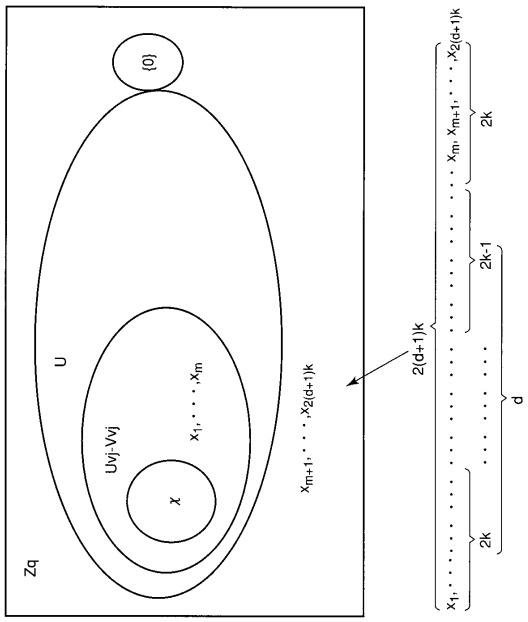
【図６】

図６



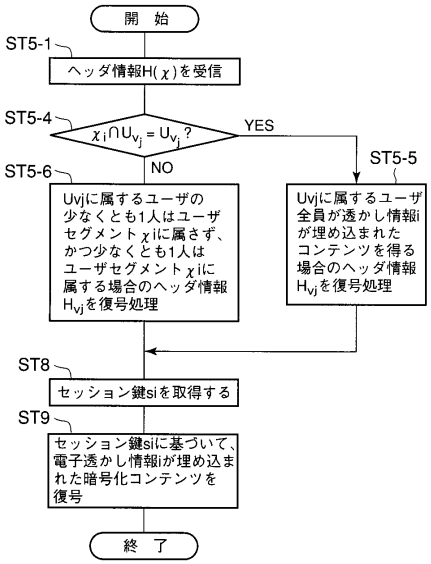
【図７】

図７



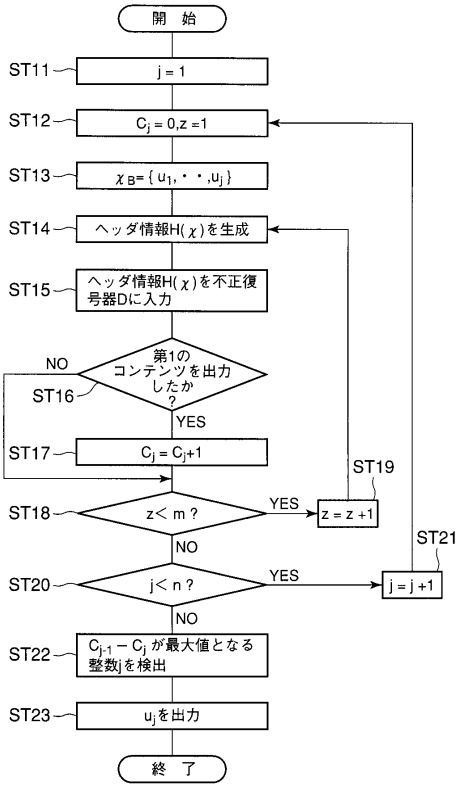
【図８】

図８



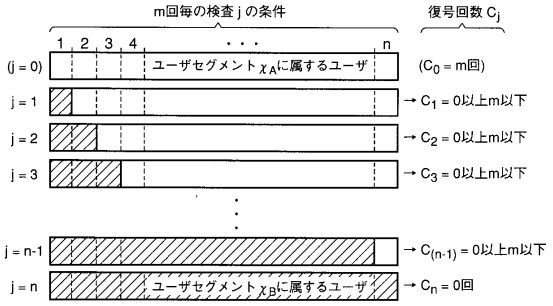
【図９】

図９



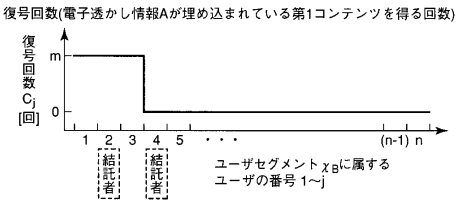
【図１０】

図１０



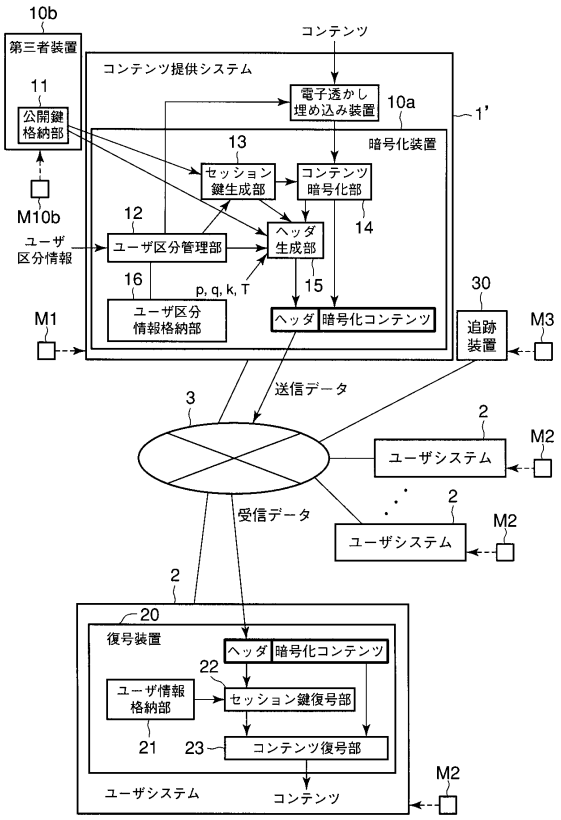
【図１１】

図１１



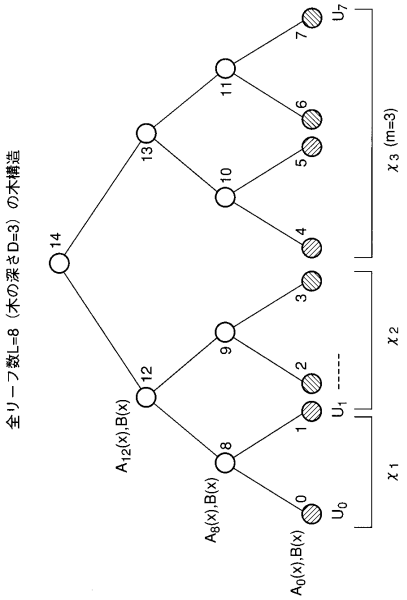
【図１２】

図 12



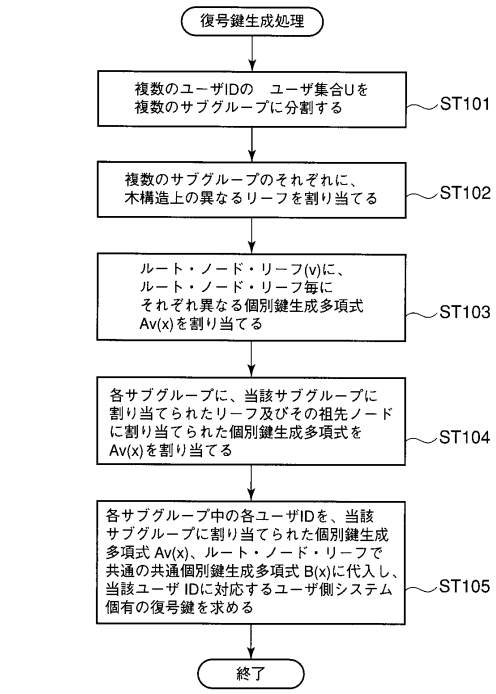
【図１３】

図 13



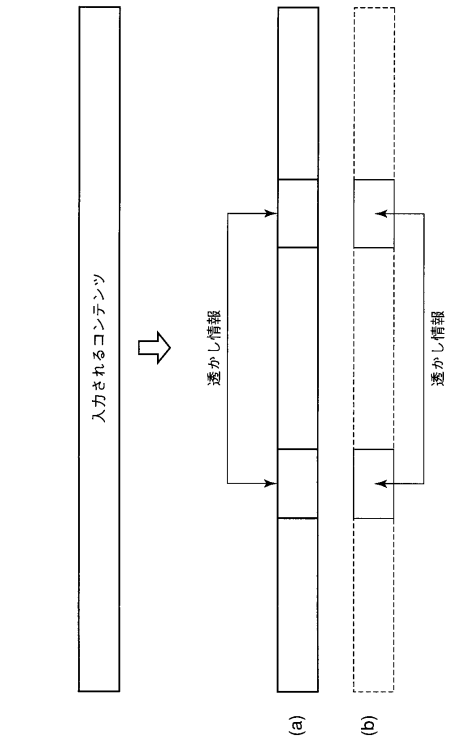
【図１４】

図 14



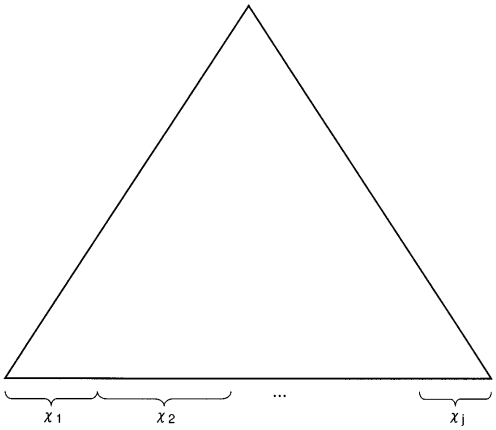
【図１５】

図 15



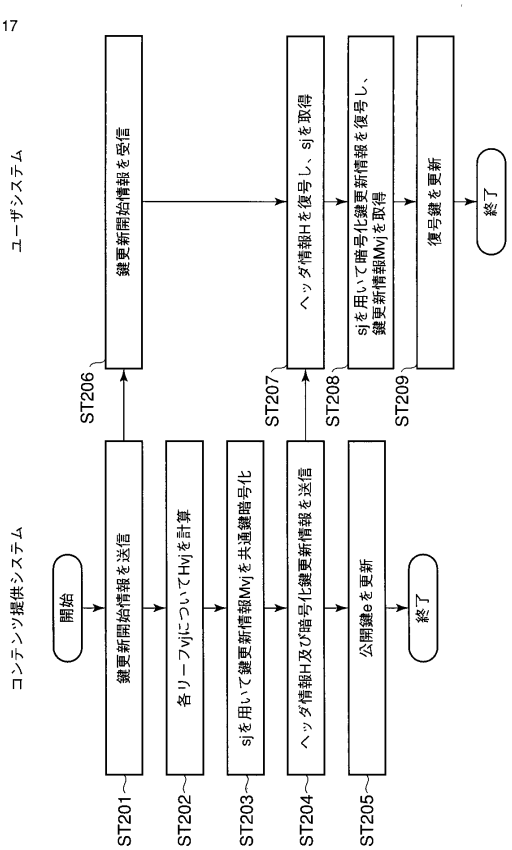
【図１６】

図 16



【図１７】

図 17



フロントページの続き

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 松下 達之
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 鳥居 稔

(56)参考文献 特開２０００－２５３４５９（ＪＰ，Ａ）
特開２００２－１６５０８１（ＪＰ，Ａ）
特開２００６－０１９９７５（ＪＰ，Ａ）
松下 達之 Tatsuyuki MATSUSHITA, より強力な不正者に対する効率的なブラックボックス追跡のための階層的な鍵割り当て Hierarchical Key Assignment for Efficient Public-Key Black-Box Tracing against Self-Defensive Pirates, 情報処理学会研究報告 Ｖｏｌ．２００６ Ｎｏ．８１ IPSJ SIG Technical Reports, 日本, 社団法人情報処理学会 Information Processing Society of Japan, ２００６年 7月２１日, 第2006巻, 頁３２１－３２８

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８