(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4630826号
(P4630826)
(45)発行日　平成23年2月9日(2011.2.9)　(24)登録日　平成22年11月19日(2010.11.19)

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

請求項の数 31　(全 46 頁)

(21)出願番号　特願2006-19795(P2006-19795)
(22)出願日　平成18年1月27日(2006.1.27)
(65)公開番号　特開2007-201950(P2007-201950A)
(43)公開日　平成19年8月9日(2007.8.9)
審査請求日　平成19年2月27日(2007.2.27)

(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　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
(74)代理人　100084618
弁理士　村松　貞男

最終頁に続く

(54)【発明の名称】復号鍵生成方法、コンテンツ提供側システム、ユーザ側システム、追跡システム、コンテンツ提供方法、暗号化コンテンツ復号方法、プログラム、暗号化装置及び復号装置

(57)【特許請求の範囲】
【請求項１】
コンテンツ提供側システムから複数のユーザ側システムへ、所定のセッション鍵で暗号化することにより得られる暗号化コンテンツと、ユーザ側システムに割り当てられたユーザ側システム固有の復号鍵を用いて前記セッション鍵を復号することを可能にするヘッダ情報とを送信し、前記暗号化コンテンツ及び前記ヘッダ情報を受信したユーザ側システムは、当該ユーザ側システムに割り当てられた復号鍵及び当該ヘッダ情報を用いて前記セッション鍵を復号し、当該セッション鍵を用いて当該暗号化コンテンツを復号するデータ通信システムにおける前記復号鍵の生成方法であって、
複数のユーザ側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を、複数のサブグループに分割する分割ステップと、
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上の異なる複数のリーフに前記複数のサブグループをそれぞれ割り当てる第１の割当ステップと、
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全部または一部のそれぞれに対し、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第２の割当ステップと、
各サブグループに対し、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つを割り当てる第３の割当ステップと、
各サブグループ中の各ユーザ識別情報を、当該サブグループに割り当てられた前記個別

鍵生成多項式と、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に代入することによって得られた値を当該ユーザ識別情報に対応するユーザ側システム固有の復号鍵とする復号鍵生成ステップと、

を含み、

前記サブグループに割り当てられた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復号鍵生成方法。

【請求項２】

前記第２の割当ステップで、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１】

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

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

（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１記載の復号鍵生成方法。

【請求項３】

前記個別鍵生成多項式A_v（ｘ）の次数k_a及び前記共有鍵生成多項式Ｂ（ｘ）の次数k_bは、最大結託人数ｋに関し、（２ｋ－１）次以上であることを特徴とする請求項２記載の復号鍵生成方法。

【請求項４】

前記第２の割当ステップで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全部または一部のそれぞれに割り当てる複数の前記個別鍵生成多項式のうち、少なくとも１つの個別鍵生成多項式の次数は、他の個別鍵生成多項式の次数とは異なることを特徴とする請求項２記載の復号鍵生成方法。

【請求項５】

前記第２の割当ステップで、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】

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

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

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

（λ_v及びc_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：予め定められた正の整数値、ｑ：予め定められた正の整数値）

であることを特徴とする請求項１記載の復号鍵生成方法。

【請求項６】

複数のユーザ側システムへ、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側システムであって、

提供すべきコンテンツをセッション鍵で復号可能に暗号化し、前記暗号化コンテンツを得るコンテンツ暗号化手段と、

前記セッション鍵を、前記複数のユーザ側システムのそれぞれに割当てられた複数の復号鍵に対応する公開鍵で暗号化し、得られた暗号化セッション鍵を含み且つ前記複数のユーザ側システムのうち前記暗号化セッション鍵の復号が許可されている各ユーザ側システム固有の復号鍵を用いて前記暗号化セッション鍵を復号することを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、

前記暗号化コンテンツ及び前記ヘッダ情報を各ユーザ側システムに送信する送信手段と、

を含み、

各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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コンテンツ提供側システム。

【請求項７】

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６記載のコンテンツ提供側システム。

【請求項８】

前記ヘッダ情報は、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固有のデータを含み、

前記ヘッダ情報生成手段は、前記複数のサブグループのうちの特定のサブグループに属する全てのユーザ側システムの復号鍵を無効にするとき、当該特定のサブグループに割り

当てられたリーフあるいは当該リーフの祖先ノードに固有のデータを正しいデータとは異なるデータに設定する、あるいは当該固有のデータを削除することを特徴とする請求項６記載のコンテンツ提供側システム。

【請求項９】

前記ヘッダ情報は、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固有のデータと、前記複数のサブグループのうちの特定のサブグループに属する複数のユーザ識別情報の部分集合に基づく値を含み、

前記ヘッダ情報生成手段は、前記特定のサブグループに属する全てのユーザ側システムのうち復号鍵を無効にするユーザ側システムのユーザ識別情報を前記部分集合に含めないことを特徴とする請求項６記載のコンテンツ提供側システム。

【請求項１０】

前記ヘッダ情報は、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固有のデータと、前記複数のサブグループのうちの特定のサブグループに属する複数のユーザ識別情報の部分集合に基づく値を含み、

前記ヘッダ情報生成手段は、前記複数のサブグループのうち前記特定のサブグループとは異なる他のサブグループに属する全てのユーザ側システムの復号鍵を無効にするとき、当該他のサブグループに割り当てられたリーフあるいは当該リーフの祖先ノードに固有のデータを正しいデータとは異なるデータに設定する、あるいは当該固有のデータを削除することを特徴とする請求項９記載のコンテンツ提供側システム。

【請求項１１】

前記ヘッダ情報生成手段は、前記木構造上の前記複数のノードのうちの１つに対応し、当該ノードを祖先ノードとする各リーフに割り当てられたサブグループに属するユーザ側システムのうち前記暗号化セッション鍵の復号が許可されているユーザ側システムに割り当てられた復号鍵を用いて前記暗号化セッション鍵を復号することを可能にする第１のヘッダ情報と、前記木構造上の前記複数のリーフのうちの１つに対応し、当該リーフに割り当てられたサブグループに属するユーザ側システムのうち前記暗号化セッション鍵の復号が許可されているユーザ側システムに割り当てられた復号鍵を用いて前記暗号化セッション鍵を復号することを可能にする第２のヘッダ情報とを生成し、

前記送信手段は、前記第１のヘッダ情報と前記第２のヘッダ情報中の各要素のうち、同一の要素を共有化して送信することを特徴とする請求項６記載のコンテンツ提供側システム。

【請求項１２】

個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システムの数が１以上である場合には、個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システムの数（ｗ）と、前記個別鍵生成多項式及び前記共通鍵生成多項式の次数との関係に基づいて設定される値ｍに関して、ｍ＋１種類のシェアデータを用いて、前記暗号化セッション鍵を復号することを可能とし、

前記ヘッダ情報生成手段は、（ａ）各ユーザ側システムに固有のシェアデータを求めるもととなる、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固有のデータと、（ｂ）個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システム固有のｗ個のシェアデータを含む、前記暗号化セッション鍵の復号が許可されている各ユーザ側システムが保持する復号鍵に依存しないｍ個のシェアデータと、を含むヘッダ情報を生成することを特徴とする請求項６記載のコンテンツ提供側システム。

【請求項１３】

前記ヘッダ情報生成手段は、個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システムの属するサブグループ以外の特定のサブグループに属する全てのユーザについて前記暗号化セッション鍵を復号不能とする場合には、当該特定のサブグループに割り当てられたリーフあるいは当該リーフの祖先ノードに固有のデータを正しいデータとは異なるデータに設定する、あるいは当該固有のデータを削除することを特徴とする請求項１２記載のコンテンツ提供側システム。

【請求項１４】
提供すべきコンテンツをセッション鍵で暗号化することにより得られる暗号化コンテンツと、暗号化されたセッション鍵を含み且つ当該暗号化されたセッション鍵を復号することを可能にするヘッダ情報とを送信するコンテンツ提供側システムから提供される前記暗号化コンテンツを復号するユーザ側システムであって、
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、複数のユーザ側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側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、当該ユーザ側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、当該ユーザ側システム固有の復号鍵を記憶する記憶手段と、
前記暗号化コンテンツ及び前記ヘッダ情報を受信する手段と、
前記復号鍵を用いて、受信した前記ヘッダ情報からセッション鍵を復号するセッション鍵復号手段と、
復号されたセッション鍵を用いて、受信した前記暗号化コンテンツを復号するコンテンツ復号手段と、
を備えたユーザ側システム。
【請求項１５】
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１４記載のユーザ側システム。
【請求項１６】
前記ヘッダ情報は、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固有のデータを含み、当該固有のデータは、前記複数のサブグループのうちの特定のサブグループに属する全てのユーザ側システムの復号鍵を無効にするとき、正しいデータとは異なるデータに設定されている、あるいは削除されており、
前記セッション鍵復号手段は、前記ヘッダ情報に含まれる、当該ユーザ側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あるいはその祖先ノードに固有のデータを用いて前記セッション鍵を復号することを特徴とする請求項１４記載のユーザ側システム。
【請求項１７】
前記ヘッダ情報は、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固有のデータと、前記複数のサブグループのうちの特定のサブグループに属する複数のユーザ識別情報の部分集合に基づくデータを含み、当該部分集合は、前記特定のサブグループに属する全てのユーザ側システムのうち復号鍵を無効にするユーザ側システムのユーザ識別情報を含まないように設定されており、
前記セッション鍵復号手段は、前記ヘッダ情報に含まれる、当該ユーザ側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あるいはその祖先ノードに固有のデータと、当該サブグループに属する複数のユーザ識別情報の部分集合に基づくデータとを用いて前記セッション鍵を復号することを特徴とする請求項１４記載のユーザ側システム。
【請求項１８】
前記複数のサブグループのうち前記特定のサブグループとは異なる他のサブグループに属する全てのユーザ側システムの復号鍵を無効にするために、当該他のサブグループに割り当てられたリーフあるいは当該リーフの祖先ノードに固有のデータを正しいデータとは

異なるデータに設定されている、あるいは当該固有のデータが削除されていることを特徴とする請求項１７記載のユーザ側システム。

【請求項１９】

前記ヘッダ情報は、

個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システムの数が１以上である場合には、個別に前記セッション鍵を復号不能とすべきユーザ側システムの数（ｗ）と、前記個別鍵生成多項式及び前記共通鍵生成多項式の次数との関係に基づいて設定される値ｍに関して、ｍ＋１種類のシェアデータを用いて、前記セッション鍵を復号することを可能にするために、（ａ）各ユーザ側システムに固有のシェアデータを求めるもととなる、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固有のデータと、（ｂ）個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システム固有のｗ個のシェアデータを含む、前記セッション鍵の復号が許可されているユーザ側システムが保持する復号鍵に依存しないｍ個のシェアデータと、を含み、

前記セッション鍵復号手段は、

前記ヘッダ情報に含まれる、当該ユーザ側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あるいはその祖先ノードに固有のデータを用いて、当該ユーザ側システムに固有のシェアデータを求め、求めたシェアデータ及び前記ヘッダ情報に含まれているｍ個のシェアデータを用いて、前記セッション鍵を復号することを特徴とする請求項１４記載のユーザ側システム。

【請求項２０】

個別に前記暗号化セッション鍵を復号不能とすべきユーザ側システムの属するサブグループ以外の特定のサブグループに属する全てのユーザについて前記暗号化セッション鍵を復号不能とするために、当該特定のサブグループに割り当てられたリーフあるいは当該リーフの祖先ノードに固有のデータを正しいデータとは異なるデータに設定されている、あるいは当該固有のデータが削除されていることを特徴とする請求項１９記載のユーザ側システム。

【請求項２１】

検査対象のユーザ側システムを検査し、複数のユーザ側システムの複数のユーザのなかから不正ユーザを特定するための追跡システムであって、

コンテンツをセッション鍵で暗号化し、暗号化コンテンツを得るコンテンツ暗号化手段と、

前記セッション鍵を暗号化することにより得られた暗号化セッション鍵を含み、当該暗号化セッション鍵の復号を許す各ユーザ側システムの復号鍵で、当該暗号化セッション鍵を復号することを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、

前記暗号化コンテンツ及び前記ヘッダ情報を前記検査対象のユーザ側システムに入力し、このユーザ側システムによる前記暗号化コンテンツの復号結果を取得する手段と、

前記暗号化セッション鍵を復号不能な無効化対象ユーザ側システムの数を変えて、前記ヘッダ情報生成手段に複数のヘッダ情報を生成させ、各ヘッダ情報と、当該ヘッダ情報を前記検査対象のユーザ側システムに入力したときに取得した復号結果との関係に基づいて、前記複数のユーザ側システムのなかから、前記検査対象のユーザ側システムの作出のもととなった１以上のユーザ側システムを特定する特定手段と、

を備え、

各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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追跡システム。

【請求項２２】

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２１記載の追跡システム。

【請求項２３】

前記特定手段は、前記無効化対象ユーザ側システムの数がｊ－１のときに復号可能と判定され、当該ｊ－１のユーザ側システムとは異なる他の１つのユーザ側システムをさらに加えた前記無効化対象ユーザ側システムの数がｊのときに復号不能と判定されたとき、当該他のユーザ側システムのユーザを不正ユーザであると特定することを特徴とする請求項２１記載の追跡システム。

【請求項２４】

複数のユーザ側システムへ、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側システムにおけるコンテンツ提供方法であって、

提供すべきコンテンツをセッション鍵で復号可能に暗号化し、前記暗号化コンテンツを得るコンテンツ暗号化ステップと、

前記セッション鍵を、前記複数のユーザ側システムのそれぞれに割り当てられた複数の復号鍵に対応する公開鍵で暗号化し、得られた暗号化セッション鍵を含み且つ前記複数のユーザ側システムのうち前記暗号化セッション鍵の復号が許可されている各ユーザ側システム固有の復号鍵を用いて前記暗号化セッション鍵を復号することを可能にするヘッダ情報を生成するヘッダ情報生成ステップと、

前記暗号化コンテンツ及び前記ヘッダ情報を各ユーザ側システムに送信する送信ステップと、

を含み、

各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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コンテンツ提供方法。

【請求項２５】

提供すべきコンテンツをセッション鍵で暗号化することにより得られる暗号化コンテンツと、暗号化されたセッション鍵を含み且つ当該暗号化されたセッション鍵を復号することを可能にするヘッダ情報とを送信するコンテンツ提供側システムから提供される前記暗号化コンテンツを復号するユーザ側システムにおける暗号化コンテンツ復号方法であって、

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、複数のユーザ側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側シス

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、当該ユーザ側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、当該ユーザ側システム固有の復号鍵を、記憶手段に記憶するステップと、

前記暗号化コンテンツ及び前記ヘッダ情報を受信するステップと、

前記復号鍵を用いて、受信した前記ヘッダ情報からセッション鍵を復号するセッション鍵復号ステップと、

復号されたセッション鍵を用いて、受信した前記暗号化コンテンツを復号するコンテンツ復号ステップと、

を含む暗号化コンテンツ復号方法。

【請求項２６】

コンテンツをセッション鍵で暗号化し、暗号化コンテンツを得るコンテンツ暗号化手段と、

前記セッション鍵を暗号化することにより得られた暗号化セッション鍵を含み、当該暗号化セッション鍵の復号を許す各ユーザ側システムの復号鍵で、当該暗号化セッション鍵を復号することを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、

前記暗号化コンテンツ及び前記ヘッダ情報を前記検査対象のユーザ側システムに入力し、このユーザ側システムによる前記暗号化コンテンツの復号結果を取得する手段と、

を備え、

検査対象のユーザ側システムを検査し、複数のユーザ側システムの複数のユーザのなかから不正ユーザを特定するための追跡システムに用いられる不正ユーザ特定方法であって、

前記暗号化セッション鍵を復号不能な無効化対象ユーザ側システムの数を変えて、前記ヘッダ情報生成手段に複数のヘッダ情報を生成させるステップと、

各ヘッダ情報と、当該ヘッダ情報を前記検査対象のユーザ側システムに入力したときに取得した復号結果との関係に基づいて、前記複数のユーザ側システムのなかから、前記検査対象のユーザ側システムの作出のもととなった１以上のユーザ側システムを特定するステップと、

を有し、

各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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不正ユーザ特定方法。

【請求項２７】

コンピュータを、複数のユーザ側システムへ、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側システムとして機能させるためのプログラムであって、

前記コンピュータは、前記プログラムを記憶する記憶手段と、前記記憶手段に接続される演算手段とを具備し、

前記演算手段は、前記記憶手段から読み出されたプログラムに従って、

提供すべきコンテンツをセッション鍵で復号可能に暗号化することにより、暗号化コンテンツを得、

前記セッション鍵を、前記複数のユーザ側システムのそれぞれに割り当てられた複数の復号鍵に対応する公開鍵で暗号化し、得られた暗号化セッション鍵を含み且つ前記複数のユーザ側システムのうち前記暗号化セッション鍵の復号が許可されている各ユーザ側システム固有の復号鍵を用いて前記暗号化セッション鍵を復号することを可能にするヘッダ情報を生成し、

前記暗号化コンテンツ及び前記ヘッダ情報を各ユーザ側システムに送信するよう構成され、

各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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プログラム。

【請求項２８】

コンピュータを、コンテンツ提供側システムから提供される暗号化コンテンツを復号するユーザ側システムとして機能させるためのプログラムであって、

前記コンピュータは、前記プログラムを記憶する記憶手段と、前記記憶手段に接続される演算手段とを具備し、

前記記憶手段は、

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、複数のユーザ側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側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、当該ユーザ側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、当該ユーザ側システム固有の復号鍵を、記憶し、

前記演算手段は、前記記憶手段から読み出されたプログラムに従って、

前記コンテンツ提供側システムから送信された、セッション鍵で暗号化された前記暗号化コンテンツと、暗号化されたセッション鍵を含み且つ当該暗号化されたセッション鍵を復号することを可能にするヘッダ情報とを受信し、

前記復号鍵を用いて、受信した前記ヘッダ情報からセッション鍵を復号し、

復号されたセッション鍵を用いて、受信した前記暗号化コンテンツを復号するように構成される、プログラム。

【請求項２９】

コンピュータを、検査対象のユーザ側システムを検査し、複数のユーザ側システムの複数のユーザのなかから不正ユーザを特定するための追跡システムとして機能させるためのプログラムであって、

前記コンピュータは、前記プログラムを記憶する記憶手段と、前記記憶手段に接続される演算手段とを具備し、

前記演算手段は、前記記憶手段から読み出されたプログラムに従って、

コンテンツをセッション鍵で暗号化し、暗号化コンテンツを得、

前記セッション鍵を暗号化することにより得られた暗号化セッション鍵を含み、当該暗

号化セッション鍵の復号を許す各ユーザ側システムの復号鍵で、当該暗号化セッション鍵を復号することを可能にするヘッダ情報を生成し、
前記暗号化コンテンツ及び前記ヘッダ情報を前記検査対象のユーザ側システムに入力し、このユーザ側システムによる前記暗号化コンテンツの復号結果を取得し、
前記暗号化セッション鍵を復号不能な無効化対象ユーザ側システムの数を変えて、前記ヘッダ情報生成手段に複数のヘッダ情報を生成させ、各ヘッダ情報と、当該ヘッダ情報を前記検査対象のユーザ側システムに入力したときに取得した復号結果との関係に基づいて、前記複数のユーザ側システムのなかから、前記検査対象のユーザ側システムの作出のもととなった１以上のユーザ側システムを特定するように構成され、
各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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プログラム。

【請求項３０】
複数のユーザ側システムへ提供する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生成する暗号化装置であって、
提供すべきコンテンツをセッション鍵で復号可能に暗号化し、前記暗号化コンテンツを得るコンテンツ暗号化手段と、
前記セッション鍵を、前記複数のユーザ側システムのそれぞれに割当てられた複数の復号鍵に対応する暗号化鍵で暗号化し、得られた暗号化セッション鍵を含み且つ前記複数のユーザ側システムのうち前記暗号化セッション鍵の復号が許可されている各ユーザ側システム固有の復号鍵を用いて前記暗号化セッション鍵を復号することを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、
を含み、
各ユーザ側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、前記複数のユーザ側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、当該ユーザ側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、当該ユーザ側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暗号化装置。

【請求項３１】
コンテンツ提供側システムから送信される、セッション鍵で暗号化することにより得られる暗号化コンテンツと、暗号化されたセッション鍵を含み且つ当該暗号化されたセッション鍵を復号することを可能にするヘッダ情報とを受信するユーザ側システムで用いられる復号装置であって、
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、複数のユーザ側システムを

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側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、当該ユーザ側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、当該ユーザ側システム固有の復号鍵を記憶する記憶手段と、

前記復号鍵を用いて、前記ヘッダ情報からセッション鍵を復号するセッション鍵復号手段と、

復号されたセッション鍵を用いて、前記暗号化コンテンツを復号するコンテンツ復号手段と、

を備えた復号装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンテンツ提供側システムから複数のユーザ側システムへ、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の不正ユーザ特定方法では、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の不正ユーザ特定方法では、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、ブラックボックス追跡が失敗するという問題がある。この問題を鑑み、特許文献１では、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】

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のうち、より効率的な送信オーバヘッドを達成している方法として、ユーザに木構造のリーフを割り当て、鍵生成多項式をマルチレベル化することにより送信データ量を削減している方法がある。ここで、製造コストなどの理由から、復号器が持つことのできるメモリサイズが制限されるため、復号器が保持すべき復号鍵データサイズをより削減したいという要求がある。従って、復号器が保持すべき復号鍵データサイズをさらに削減することが望ましい。

【特許文献１】特開２００５－２３６９６３号公報

【発明の開示】

【発明が解決しようとする課題】

【００１２】

以上説明したように従来の不正ユーザ特定方法では、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えること、及び、そのために復号器が保持すべき復号鍵データサイズの削減を図ること、という２つの課題を解決することはできない問題点があった。

【００１３】

そこで、本発明は、上記問題点に鑑みなされたもので、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、巧妙な不正復号器に対しても、確実に追跡を実行し得、しかも、復号器が保持すべき復号鍵データサイズの削減を図ることができる復号鍵生成方法、コンテンツ提供側システム、ユーザ側システム、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】

【００１４】

コンテンツ提供側システムから複数のユーザ側システムへ、所定のセッション鍵で暗号化することにより得られる暗号化コンテンツと、ユーザ側システムに割り当てられたユーザ側システム固有の復号鍵を用いて前記セッション鍵を復号することを可能にするヘッダ情報とを送信し、前記暗号化コンテンツ及び前記ヘッダ情報を受信したユーザ側システムは、当該ユーザ側システムに割り当てられた復号鍵及び当該ヘッダ情報を用いて前記セッション鍵を復号し、当該セッション鍵を用いて当該暗号化コンテンツを復号するデータ通信システムにおいて、各ユーザ側システム固有の前記復号鍵は、

複数のユーザ側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を、複数のサブグループに分割し、

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上の異なる複数のリーフに前記複数のサブグループをそれぞれ割り当てるとともに、

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全部または一部のそれぞれに対し、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、
各サブグループに対し、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つを割り当て、
各サブグループ中の各ユーザ識別情報を、当該サブグループに割り当てられた前記個別鍵生成多項式と、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に代入することによって得られた値を当該ユーザ識別情報に対応するユーザ側システム固有の復号鍵とし、
前記サブグループに割り当たられた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。

【００１５】

各ユーザ側システムは、サブグループ単位に木構造上のリーフに割り当てられ、各木構造上のリーフ、その祖先ノードにより分類、識別される。従って、ヘッダ情報には、ユーザ側システムのユーザ識別情報を含まれていないので、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、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、木構造上の複数のノード及び複数のリーフに共通な共通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、送信オーバヘッドを同程度に保ちつつ、復号器が保持すべき復号鍵データサイズの削減が可能となる。

【発明の効果】

【００１６】

以上説明したように本発明によれば、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、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、復号器が保持すべき復号鍵データサイズの削減が可能となる。

【発明を実施するための最良の形態】

【００１７】

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側システム及びユーザ側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集合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。

【００１８】

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を有するコンテンツ提供側システム１と、復号装置２０を有するｎ個のユーザ側システム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。

【００１９】

ここで、コンテンツ提供側システム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。

【００２０】

ｎ個のユーザ側システム２は、コンテンツ提供側システム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。

【００２１】

なお、図１では、１つのコンテンツ提供側システム１のみ示しているが、コンテンツ提供側システム１が複数存在しても構わない。

【００２２】

また、１つのノードが、コンテンツ提供側システム１の機能とユーザ側システム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側システム１の機能とユーザ側システム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。

【００２３】

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。

【００２４】

次に、コンテンツ提供側システム１に搭載される暗号化装置１０を説明する。

暗号化装置１０は、公開鍵格納部１１、無効化対象ユーザ情報格納部１２、セッション鍵生成部１３、コンテンツ暗号化部１４及びヘッダ生成部１５を備えている。

【００２５】

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。

【００２６】

無効化対象ユーザ情報格納部１２は、無効化の対象とするユーザに関する情報（ユーザＩＤ等）を格納するメモリであり、ヘッダ生成部１５から読出可能となっている。

【００２７】

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セッション鍵を生成する機能をもっている。

【００２８】

コンテンツ暗号化部１４は、提供すべきコンテンツを、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暗号化し、暗号化コンテンツを得る機能をもっている。なお、暗号化コンテンツはセッション鍵に基づいて復号可能である。

【００２９】

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の）情報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機能をもっている。

【００３０】

具体的には、ヘッダ生成部１５は、暗号化セッション鍵及び３種類のヘッダ情報を生成する機能を有する。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。

【００３１】

第１のヘッダ情報は、無効化対象ユーザに関するものであり、暗号化セッション鍵を含まないものである。

【００３２】

第２のヘッダ情報は、無効化対象ユーザ及び有効化対象ユーザに関する。第２のヘッダ情報は、セッション鍵を公開鍵で暗号化し、得られた暗号化セッション鍵を含み且つ暗号化セッション鍵の復号を許す各ユーザ側システムのうち少なくとも１つのユーザ側システムのユーザ識別情報に基づく値を含んでいる。なお、暗号化セッション鍵は復号鍵に基づいて復号可能である。

【００３３】

第３のヘッダ情報は、有効化対象ユーザに関するものであり、暗号化セッション鍵を含んでいる。なお、第３のヘッダ情報は、有効化対象ユーザのユーザ識別情報に基づく値を含まない。但し、第３のヘッダ情報は、有効化対象ユーザのユーザ識別情報に基づく値を含んでもよい。

【００３４】

なお、コンテンツ提供側システム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、コンテンツ提供側システム１は、複数のサブグループ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。

【００３５】

ここで、復号鍵生成装置は、各ユーザ側システム固有の復号鍵を生成するものであり、複数のユーザ側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が属するグループ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、ユーザ側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側システム固有の復号鍵とする機能とをもっている。

【００３６】

詳しくは、ユーザの復号鍵は鍵生成多項式にユーザ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１５に示すように全ユーザ集合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１５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。

【００３７】

図１５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１５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１５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。

【００３８】

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。

【００３９】

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。

【００４０】

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。

【００４１】

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。

【００４２】

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る割り当て方とし、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１５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。

【００４３】

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。

【００４４】

なお、ユーザ側システム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側システム１または信頼できる第三者からユーザ側システム２へ与えられて保持しておくものとする。

【００４５】

なお、図１５、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。

【００４６】

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。

【００４７】

次に、ユーザ側システム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。

【００４８】

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。

【００４９】

セッション鍵復号部２２は、コンテンツ提供側システム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）する機能をもっている。

【００５０】

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、コンテンツ提供側システム１から受信した暗号化コンテンツを復号する機能をもっている。

【００５１】

なお、ユーザ側システム２は、コンテンツ提供側システム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。

【００５２】

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及び制御部３３を備えている。

【００５３】

ここで、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。

【００５４】

ヘッダ生成部３２は、制御部３３から指示された無効化対象ユーザ集合に従い、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、前述同様に、ユーザ側システム固有の復号鍵で復号可能に暗号化されたセッション鍵を含み且つ当該暗号化されたセッション鍵の復号を許可する各ユーザ側システムの各ユーザ識別情報に基づく値を含むように生成される。

【００５５】

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の制御により、復号不能なユーザ側システムの数を変えて生成されたヘッダ情報と、当該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側システムの作出のもととなった１又は複数のユーザ側システムの不正ユーザを特定する機能をもっている。

【００５６】

詳しくは制御部３３は、無効化すべき（１又は複数の）ユーザＩＤ（すなわち無効化対象ユーザ集合χ）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により復号されたセッション鍵を入力し、正しいセッション鍵が得られたか否かを調べる機能と、無効化対象ユーザ集合を変えながら、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ＩＤを特定する機能とをもっている。

【００５７】

なお、制御部３３は、検査対象復号装置２０χによるセッション鍵の復号結果（正しいセッション鍵が得られた否か）を判断しているが、これに限らず、ヘッダ情報に加え、セッション鍵で暗号化されたコンテンツを検査対象復号装置２０χに入力し、検査対象復号装置２０χによるコンテンツの復号結果（コンテンツが復号されたか否か）を判断してもよい。

【００５８】

また、追跡装置３０は、例えば、コンテンツ提供側システム１に搭載されてもよいし、コンテンツ提供側システム１とは独立した装置であってもよい。また、ネットワーク３に接続する機能を備えてもよいし、備えなくても構わない。

【００５９】

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。

【００６０】

各ユーザ側システム２には、それぞれ固有のユーザＩＤが割り当てられているとする。

【００６１】

コンテンツ提供側システム１は、所定のセッション鍵（単一の鍵）ｓを生成し（ＳＴ１）、無効化対象のユーザ集合に応じてセッション鍵を暗号化し、ヘッダ情報Ｈ（χ）を生成する（ＳＴ２）。

【００６２】

次に、コンテンツ提供側システム１は、該セッション鍵ｓでコンテンツを暗号化し（ＳＴ３）、得られた暗号化コンテンツに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（ＳＴ４）。

【００６３】

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、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）。

【００６４】

各々のユーザ側システム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、無効化対象のユーザ集合χとの関係に応じて、ヘッダ情報を復号処理する（ＳＴ５）。

【００６５】

ここで、各々のユーザ側システム２は、無効化対象のユーザ集合χに属していれば（ＳＴ６）、セッション鍵を取得できない（ＳＴ７）。逆に、無効化対象のユーザ集合χに属していなければ（ＳＴ６）、セッション鍵を取得し（ＳＴ８）、セッション鍵で暗号化コンテンツを復号する（ＳＴ９）。

【００６６】

また、詳しくは後述するように、コンテンツ提供側システム１は、無効化対象のユーザ集合χに応じてヘッダ情報を生成するので、復号鍵を柔軟に無効化できる。復号鍵の無効化は、無効化対象ユーザの復号鍵を用いてもセッション鍵が得られず、かつそれ以外のユーザの復号鍵で復号できる形式に、セッション鍵を暗号化することにより達成される。

【００６７】

なお、放送型コンテンツ配信では、送信データは単一のセッション鍵で暗号化されるのが一般的であり、鍵配送方法とは、セッション鍵を各ユーザの復号鍵で復号できる形式に暗号化するセッション鍵の暗号化・復号方法を意味する。

【００６８】

さて、以下では、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～ＳＴ８の復号フェーズについて、詳細に説明する。

【００６９】

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。

【００７０】

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。

ユーザＩＤ（ユーザ番号）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。

無効化対象ユーザ集合（復号鍵を無効化されるユーザの集合）をχとする。

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。

【００７１】

（鍵生成フェーズ）

本実施形態では、分割した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ている。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。

【００７２】

ここでは、公開鍵及び各ユーザＩＤに対応するユーザ側システムの復号鍵の生成処理に

ついて説明する。なお、図１６に示すフローチャートには、各ユーザＩＤに対応するユーザ側システムの復号鍵の生成処理を示している。

【００７３】

コンテンツ提供側システム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、分割サブグループ数をＬとし、Ｌは２のべき乗で表される数とする。コンテンツ提供側システム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。

【００７４】

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。

【００７５】

次に、コンテンツ提供側システム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３】

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

【００７６】

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１５の例では、Ｎ＝｛０、…１３｝である。

【００７７】

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。

【００７８】

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）。

【００７９】

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１５では、例えば、$U_8=U_0+U_1$である。ここで、＋は和集合を表す。

【００８０】

最後にコンテンツ提供側システム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。

【数４】

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

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

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

【００８１】

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。

【００８２】

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。

【００８３】

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］＋［λ_iＢ（ｘ）のｍ次係数］は、ｉ、ｊによらず一定である。

【００８４】

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）＋λ_iＢ（ｘ）の「ｘ」に「ｕ」を代入することにより得られる。

【００８５】

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。

【００８６】

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５】

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

【００８７】
図１５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６】

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

【００８８】
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、コンテンツ提供側システム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。これらは以下の各実施形態でも同様である。
【００８９】
（暗号化フェーズ）
コンテンツ提供側システム１のセッション鍵生成部１３は、セッション鍵ｓをＧｑからランダムに選択する。次に、ヘッダ生成部１５は、整数ｊ＝０とし、v_0に木構造Ｔにおけるルートの子ノードのいずれかのノードＩＤを代入し、以下の処理をｊについて繰り返す。
【００９０】
v_jがリーフＩＤである場合、v_jの兄弟リーフのＩＤをv_{j+1}に代入して終了する。そうでない場合、v_jの兄弟ノードの子ノードのいずれかを選択し、そのノードＩＤをv_{j+1}に代入し、ｊを１だけインクリメントする。
【００９１】
上記処理終了後、２つのリーフＩＤを含めた$\log_2 L+1$個のノードＩＤが選択されている。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。図１５では、４つ（例えば、０、１、９、１３）のノードＩＤが選択される。
【００９２】
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、以下の処理を繰り返し、Hv_0、…、Hv_βを計算する（図６のＳＴ２－１～ＳＴ２－８）。
【００９３】
ヘッダ生成部１５は、無効化対象ユーザ集合χとU_jとの積集合が空集合であるか否かを判定する（ＳＴ２－２）。
【００９４】
ここで、χとUv_jとの積集合が空集合である場合を述べる。これは、Uv_jに属するユーザ全員が無効化対象ユーザではない場合であり、例えば、図２のU_3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（ＳＴ２－３）。

【数７】

$$H_{v_j} = (h_{v_j}, h'_{v_j}, h_{v_j,0}, \ldots, h_{v_j,y_{v_j}}, \ldots, h_{v_j,2k-1})$$

$$= (g^r, g^{\lambda_{v_j} r}, g^{ra_0}, \ldots, sg^{rc_{v_j}}, \ldots, g^{ra_{2k-1}})$$

$$y_{v_j} = v_j \bmod 2k \qquad (5)$$

【００９５】

例えば、ステップＳＴ２－２、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。

【００９６】

ステップＳＴ２－２の結果、無効化対象ユーザ集合χとUv_jとの積集合が空集合でない場合、ヘッダ生成部１５は、χとUv_jの積集合がUv_jであるか否かを判定する（ＳＴ２－４）。

【００９７】

ここで、χとUv_j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無効化対象ユーザである場合、例えば、図２のU_1が対応する。ヘッダ生成部１５は、ｒにr_0、r_1のどちらかを代入し、乱数z_{v_j}を選択する。ステップＳＴ２－５では、Uv_j以外のユーザ集合に無効化対象ユーザが含まれていない場合、すなわち、当該Uv_j以外のユーザ集合に、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、式（６）に従いHv_jを計算する（ＳＴ２－５）。

【数８】

$$H_{v_j} = (g^r, g^{\lambda_{v_j} r}, g^{ra_0}, \ldots, g^{z_{v_j}}, \ldots, g^{ra_{2k-1}}) \qquad (6)$$

【００９８】

また、Uv_j以外のユーザ集合に無効化対象ユーザが含まれている場合、すなわち、当該Uv_j以外のユーザ集合に、ステップＳＴ２－４の結果がそれ以外となる場合（ＳＴ２－４；ＮＯ）が存在すると判明している場合、式（７）に従いHv_jを計算する（ＳＴ２－５）。

【数９】

$$H_{v_j} = (h_{v_j}, h'_{v_j}, h_{v_j,0}, \ldots, h_{v_j,y_{v_j}}, \ldots, h_{v_j,2k-1})$$

$$= \begin{cases} (g^{r_0}, g^{\lambda_{v_j} r_0}, g^{r_0 a_0}, \ldots, g^{z_{v_j}}, \ldots, g^{r_0 a_{2k-1}}) & (r = r_0) \\ (g^{r_1}, g^{\lambda_{v_j} r_1}, g^{L_0 g^{r_1 a_0}}, \ldots, g^{z_{v_j}}, \ldots, g^{L_{2k-1} g^{r_1 a_{2k-1}}}) & (r = r_1) \end{cases} \qquad (7)$$

【００９９】

どちらでもない場合（ステップＳＴ２－４の結果がこの時点で不明な場合）、ｒにr_0を代入し、式（６）に従いHv_jを計算する（ＳＴ２－５）。

【０１００】

なお、式（６）、式（７）の例は、特定のサブグループUv_jに属する全てのユーザ側システム２の復号鍵を無効にするとき、ヘッダ情報Hv_jにおける特定のサブグループUv_jに固有の値c_{vj}を正しい値とは異なる値z_{vj}に設定する例である。これに限らず、例えば、無効化するサブグループについては、ヘッダ情報Hv_jにおける特定のサブグループUv_jに固有の要素であり、セッション鍵を計算するもととなる情報$h_{vj,yvj}$を削除（記述を禁止）してもよい。

【０１０１】

このようにしても、無効化するサブグループについては、ヘッダ情報に、セッション鍵を計算するもととなる情報自体が含まれていないので、結局、正しいセッション鍵を求めることができず、他方、それ以外のサブグループについては、正しいセッション鍵を求めることができることになる。

【０１０２】

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人は無効化対象ユーザではなく、かつ少なくとも１人は無効化対象ユーザである場合、例えば、図２のU_2に対応する。

【０１０３】

ヘッダ生成部１５は、図７（ｄ＝０）に示すように、Uv_jから、無効化対象ユーザ集合χを取り除いた部分集合を$\{x_1, \cdots, x_m\}$とする。例えば、図２のU_2の場合に$\{x_1, \cdots, x_{10}\} = \{31, \cdots, 40\}$（ｍ＝１０）などとなる。

【０１０４】

次に、ヘッダ生成部１５は、２ｋ－ｍ－１＞０ならば、$x_{m+1}, \cdots, x_{2k-1}$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。

【０１０５】

ヘッダ生成部１５は、$1 \leqq t \leqq 2k-1$について、式（８）を満たすＺｑの要素$L_0, \cdots, L_{2k-1}$を求める。

【数１０】

$$\sum_{i=0}^{2k-1} L_i X_t^i = 0 \bmod q \qquad (8)$$

【０１０６】

次に、ヘッダ生成部１５は、ｒにr_1を代入し、式（９）に従いHv_jを計算する（ＳＴ２－６）。

【数１１】

$$H_{v_j} = (h_{v_j}, h'_{v_j}, h_{v_j,0}, \ldots, h_{v_j,y_{v_j}}, \ldots, h_{v_j,2k-1})$$

$$= (g^r, g^{\lambda_{v_j} r}, g^{L_0} g^{r a_0}, \ldots, s g^{L_{y_{v_j}}} g^{r c_{v_j}}, \ldots, g^{L_{2k-1}} g^{r a_{2k-1}}) \qquad (9)$$

【０１０７】

ヘッダ生成部１５は、特定のサブグループに属する全てのユーザ側システムのうち、１以上のユーザ側システム２の復号鍵を無効にするとき、当該無効にするユーザ側システム２のユーザＩＤを、Uvjに属するユーザ集合のうち無効化対象ユーザでないユーザの集合である部分集合$\{x_1 \sim x_m\}$に含めないようにすればよい。

【０１０８】

なお、部分集合に基づく値$\{L_0, \cdots, L_{2k-1}\}$は、当該部分集合に属する各ユーザＩＤ$\{x_1, \cdots, x_m\}$を２ｋ－１次多項式の変数として第２ベクトルとする場合の当該第

２ベクトルとの内積を「０」とする下記式の関係を満たす第１ベクトルである。

【０１０９】

$$(L_0, L_1, L_2, \cdots, L_{2k-1}) \cdot (1, x_w, x_w^2, \cdots, x_w^{2k-1}) = 0 \mod q$$

但し、$x_w = x_1 \sim x_m$のいずれかである。

【０１１０】

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）の範囲までのｍの値を許容できる。

【０１１１】

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、これに限らす、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。これは、後述する他の実施形態においても同様である。

【０１１２】

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側システム１を運営することができる。

【０１１３】

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。

【０１１４】

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、以下に説明する方法によりノードを選択してもよい。

【０１１５】

以下、図１４を用いて説明する。始めに、ヘッダ生成部１５は、ノードv_jとしてルートＲを設定する（ＳＴ３１）。ノードv_jを祖先に持つ全ユーザについて、次の場合（１）～（３）のいずれかに該当するか否かを判定する（ＳＴ３２）。（１）全員無効化対象である場合。（２）全員有効化対象である場合。（３）有効化対象ユーザ数が１以上２ｋ－１以下である場合。

【０１１６】

ヘッダ生成部１５は、判定結果に基づいて、ヘッダHv_jを計算する（ＳＴ３３）。それぞれの場合におけるヘッダHv_jの計算は前述したものと同様である。

【０１１７】

上記（１）～（３）のいずれにも該当しない場合（ＳＴ３２；Ｎｏ）、当該ノードv_jの子ノードで、未検査の子ノードをノードv_jとして設定し（ＳＴ３４）、上記処理を繰り返す。なお、ノードv_jとしてリーフを設定しても構わない。

【０１１８】

全ての有効化対象ユーザ集合についてHv_jを生成したか否かを判定し（ＳＴ３５）、全ての有効化対象ユーザ集合についてHv_jを生成した場合、生成された（複数の）Hv_jをヘッダＨ(x)とする（ＳＴ３６）。そうでない場合（ＳＴ３５；Ｎｏ）、未検査のノードで、ルートＲに最も近い、つまり最上位のノードをノードv_jとして設定し（ＳＴ３７）、上記処理を繰り返す。なお、ノードv_jとしてリーフを設定しても構わない。

【０１１９】

上記の例では、ヘッダサイズをより削減するために、なるべく上位のノードを選択する方法を説明したが、ノードの選択方法はこれに限らず、例えば、以下のような選択方法も可能である。

【０１２０】

図１３において、U_0に属するユーザ全員が無効化対象であり、U_1に属するユーザの内

ｋ人が有効化対象であり、U_2に属するユーザ全員が有効化対象であり、U_3に属するユーザ全員が有効化対象である場合、図１４のフローチャートに従うと，ノードｊとノードｖが選択され、$H(x)=(H_j, H_v)$となる。ここで、ノードｊはリーフｉ（U_0に対応）及びリーフｗ（U_1に対応）の親ノードである。ノードｖはU_2に対応するリーフ及びU_3に対応するリーフの親ノードである。但し、これに限らず、ステップＳＴ３２の条件が満たされていれば、ノードをどう選択しても良い。例えば、リーフｉとリーフｗとノードｖを選択しても良い。このとき$H(x)=(H_i, H_w, H_v)$となる。このように、ノードの選択方法として種々の方法を用いることができることは後述する他の実施形態においても同様である。

【０１２１】

（復号フェーズ）

部分集合Uv_jに属するユーザｕを考える。ユーザＩＤ＝ｕのユーザ側システム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１２】

$$s = \left(\frac{h_{v_j,0} \times \cdots \times h_{v_j,2k-1}^{u^{2k-1}}}{h_{v_j}^{A_{v_j}(u)} h'^{B(u)}_{v_j}} \right)^{1/u^{y_{v_j}}}$$

$$= \left(\frac{s^{u^{v_j} \bmod 2k} \; g^{r\sum_{i=0}^{2k-1} a_{v_j,i} u^i}}{g^{r(A_{v_j}(u)+\lambda_{v_j}B(u))}} \right)^{1/u^{y_{v_j}}} \qquad (10)$$

$$= \left(s^{u^{v_j} \bmod 2k} \right)^{1/u^{y_{v_j}}}$$

【０１２２】

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。

ユーザ側システム２のセッション鍵復号部２２における復号結果は、無効化対象ユーザ集合χとUv_jの積集合が空集合であるか（ＳＴ５－２）、無効化対象ユーザ集合χとUv_jの積集合がUv_jであるか（ＳＴ５－４）、またはそれ以外（ＳＴ６）の場合によって場合分けされる。なお、ユーザ側システム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。

【０１２３】

ここで、χとUv_jの積集合が空集合である場合（ＳＴ５－２；ＹＥＳ）を述べる。これは、Uv_jに属するユーザ全員が無効化対象ユーザではない場合であり、例えば、図２のU_3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（ＳＴ５－３）、セッション鍵ｓを得る（ＳＴ８）。

【０１２４】

ここで、無効化対象ユーザ集合χとUv_jの積集合がUv_jである場合（ＳＴ５－４；ＹＥＳ）を述べる。これは、Uv_jに属するユーザ全員が無効化対象ユーザである場合であり、

例えば、図２のU_1が対応する。この場合、ヘッダ情報Hv_jにおける特定のサブグループUv_jに固有の要素であり、セッション鍵を計算するもととなる情報$h_{v_j,y_{v_j}}$が間違った値になっているので（ＳＴ５－５）、正しいセッション鍵を取得することができない（ＳＴ７）。

【０１２５】

ここで、それ以外の場合を述べる（ＳＴ５－４；ＮＯ）。これは、Uv_jに属するユーザの少なくとも１人は無効化対象ユーザではなく、かつ少なくとも１人は無効化対象ユーザである場合であり、例えば、図２のU_2が対応する。

【０１２６】

セッション鍵ｓは式（１１）のように表される。

【数１３】

$$s = \left(\frac{h_{v_j,0} \times \cdots \times h_{v_j,2k-1}^{u^{2k-1}}}{h_{v_j}^{A_{v_j}(u)}\, h_{v_j}^{\prime B(u)}} \right)^{1/u^{y_{v_j}}}$$

$$= \left(\frac{s^{u^{v_j \bmod 2k}}\, g^{\sum_{i=0}^{2k-1}(L_i + r_1 a_{v_j,i})u^i}}{g^{r(A_{v_j}(u) + \lambda_{v_j} B(u))}} \right)^{1/u^{y_{v_j}}} \qquad (11)$$

$$= \left(s^{u^{v_j \bmod 2k}} \right)^{1/u^{y_{v_j}}}$$

【０１２７】

ユーザｕが無効化対象ユーザである場合（ＳＴ６；ＹＥＳ）、式（１２）が不成立であるので、セッション鍵ｓを得られない（ＳＴ７）。

【数１４】

$$\sum_{i=0}^{2k-1} L_i u^i = 0 \bmod q \qquad (12)$$

【０１２８】

（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。

【０１２９】

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。

【０１３０】

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。

【０１３１】

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。

【０１３２】

（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。

【０１３３】

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。

【０１３４】

なお、木構造Ｔにおいて、各リーフには２ｋ人のユーザが属しているとし、各リーフＩＤを、一番左のリーフから１、…、ｔとし、部分集合U_1、…、U_tの要素は、式（１３）のようにラベル付けされているとする。

【数１５】

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

【０１３５】

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、正常な復号回数C_j＝０、同一の無効化対象ユーザ集合χの検査回数ｚ＝１と代入し、以下の処理をｍ回繰り返す（ＳＴ１２）。

【０１３６】

制御部３３は、無効化対象ユーザ集合χ＝｛u_1、…、u_j｝とし（ＳＴ１３）、ヘッダ生成部３２を制御し、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。ただし、ノードの選択に際して、以下の条件（１）、（２）をともに満たす$\log_2 L + 1$個のノードv_jを選択する。（１）Uv_jからχを除いた集合の要素数が「１」以上「２ｋ」未満である、又は、Uv_jとχの積集合が空集合である、又は、Uv_jとχの積集合がUv_jである。（２）Uv_jからχを除いた集合の要素数が「１」以上「２ｋ」未満であるノードは高々１個である。

【０１３７】

ヘッダ生成部３２がヘッダＨ（χ）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。

【０１３８】

このとき、制御部３３は、不正復号器Ｄが正しいセッション鍵ｓを出力したか否かを判定し（ＳＴ１６）、正しいセッション鍵ｓ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）。そうでない場合（ＳＴ１６；ＮＯ）、C_jの値を変化させない。

【０１３９】

なお、不正復号器Ｄが復号後のコンテンツのみを出力する場合、コンテンツが正しく復号されているか否かを観測し、コンテンツが正しく復号されていれば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。

【０１４０】

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。

【０１４１】

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、無効化対象のユーザ番号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。

【０１４２】

ステップＳＴ２０の判定の結果、無効化対象のユーザ番号ｊがユーザ総数ｎに一致すると検査が終了する。

【０１４３】

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）。

【０１４４】

この追跡方法では、図１０及び図１１に示すように、無効化対象ユーザ集合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無効化したときに復号不能となるかを検査しており、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。

【０１４５】

例えば、ユーザＩＤの集合を$\{u_1、\cdots、u_n\}$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。

【０１４６】

この場合、ユーザＩＤ＝u_1、u_2、u_3を無効化対象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、正しいセッション鍵が得られるので、ｍ回の繰り返し処理後C_3＝ｍとなる。

【０１４７】

また、ユーザＩＤ＝u_1、u_2、u_3、u_4を無効化対象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、正しいセッション鍵が得られないので、ｍ回の繰り返し処理後C_4＝０となる。

【０１４８】

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。

【０１４９】

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。

【０１５０】

なお、検査対象復号装置がより巧妙な不正復号器であるとき、検査対象復号装置がブラックボックス追跡を検知して、ある時点以降、ヘッダ生成部３２からの入力を全く受け付けなくなる場合が考えられる。この場合、その時点のｊの値を用いて不正ユーザＩＤをu_jと特定できる。これは以下の各実施形態でも同様である。

【０１５１】

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。

【０１５２】

上述したように本実施形態によれば、ヘッダ情報が、ユーザ側システムのユーザ識別情報を含まないので、ブラックボックス追跡の際に、誰の復号鍵が無効化されているかとい

う情報が漏れない。これにより、ブラックボックス追跡の際に、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。

【０１５３】

また、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、本実施形態では、一方の鍵生成多項式Ｂ（ｘ）を全ノードに対し共通としているため、送信オーバヘッドを同程度に保ちつつ、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。

【０１５４】

（第２の実施形態）

次に、本発明の第２の実施形態について説明する。本実施形態は、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、χとUv_jの積集合がUv_jでない場合（ＳＴ２－４；ＮＯ）、鍵生成多項式の次数を増やすことなく、ｍ＜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χとUv_jの積集合がUv_jでない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。

【０１５５】

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。

【０１５６】

（暗号化フェーズ）

ステップＳＴ２－４において、χとUv_jの積集合がUv_jでない場合（ＳＴ２－４；ＮＯ）について述べる。

【０１５７】

ヘッダ生成部１５は、図７に示すように、Uv_jから、無効化対象ユーザ集合χを取り除いた部分集合を｛x_1、…、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、無効化対象でないユーザ（有効ユーザ）の総数である。

【０１５８】

次に、ヘッダ生成部１５は、$2dk \leqq m \leqq 2dk+2k-1$を満たす整数ｄを探し、$2dk+2k-m-1>0$ならば、$x_{m+1}$、…、$x_{2dk+2k-1}$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。

【０１５９】

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

【数１６】

$$\sum_{i=0}^{2dk+2k-1} L_i x_t^i = 0 \bmod q \qquad (14)$$

【０１６０】

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１７】

$$H_{v_j} = \left(h_{v_j}, h'_{v_j}, h_{v_j,0}, \cdots, h_{v_j,2dk+2k-1} \right)$$

$$h_{v_j} = g^r$$

$$h'_{v_j} = g^{\lambda_{v_j} r}$$

$$h_{v_j,i} = \begin{cases} g^{L_i} g^{r a_{i \bmod 2k}} & (y_{v_j} \neq i \bmod 2k) \\ s g^{L_i} g^{r c_{v_j}} & (y_{v_j} = i \bmod 2k) \end{cases}$$

$$y_{v_j} = v_j \bmod 2k \qquad (15)$$

【０１６１】

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。

【０１６２】

（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１８】

$$s = \left(\frac{h_{v_j,0} \times \cdots \times h_{v_j,2dk+2k-1}^{u^{2dk+2k-1}}}{\left(h_{v_j}^{A_{v_j}(u)} h'^{B(u)}_{v_j} \right)^{\sum_{t=0}^{d} u^{2kt}}} \right)^{1/u^{y_{v_j}\left(\sum_{t=0}^{d} 2kt+1\right)}}$$

$$= \left(\frac{s^{u^{y_{v_j}\left(\sum_{t=0}^{d} 2kt+1\right)}} g^{\sum_{i=0}^{2dk+2k-1} L_i u^i} \left(g^{\sum_{i=0}^{2k-1} r_1 a_{v_j,i} u^i} \right)^{\sum_{t=0}^{d} u^{2kt}}}{g^{r1\left(A_{v_j}(u)+\lambda_{v_j} B(u)\right)\sum_{t=0}^{d} u^{2kt}}} \right)^{1/u^{y_{v_j}\left(\sum_{t=0}^{d} 2kt+1\right)}}$$

$$= \left(s^{u^{v_j \bmod 2k}} \right)^{1/u^{y_{v_j}}}.$$

(16)

【０１６３】

ユーザｕが無効化対象ユーザである場合（ＳＴ６；ＹＥＳ）、式（１７）が不成立であるので、セッション鍵ｓを得られない（ＳＴ７）。

【数１９】

$$\sum_{i=0}^{2dk+2k-1} L_i u^i = 0 \bmod q \qquad (17)$$

【０１６４】

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、あるサブグループUv_jに、無効化対象ユーザと、無効化対象でない有効ユーザとが共存する場合に、有効ユーザの数を第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「２ｄｋ＋２ｋ－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「２ｄｋ＋２ｋ＋２」に増えている）。

【０１６５】

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、有効化対象ユーザ数が第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。

【０１６６】

（第３の実施形態）

次に、本発明の第３の実施形態について説明する。本実施形態は、第１の実施形態と特許文献２（特開２００３－２８９２９６）において開示されている復号鍵無効化方法を組み合わせた例である。

【０１６７】

すなわち、例えば、図１７（ａ）（なお、図１７（ａ）（ｂ）（ｃ）において、下線が無効化対象ユーザを示す）に示すように、ユーザＩＤ＝１、２、３のみを無効化する場合には、ある４つのデータ（後述するシェア）が揃って初めて、セッション鍵を復号できるようにする（説明を簡単にするため、無効化対象ユーザ数と最大結託人数が等しいとすると、無効化対象ユーザ数＋１のシェアが揃って初めて、セッション鍵を復号できるようにする）。

【０１６８】

ヘッダ情報には、ユーザＩＤ＝１について求まるシェア（１，$g^{F(1)}$）、ユーザＩＤ＝２について求まるシェア（２，$g^{F(2)}$）、ユーザＩＤ＝３について求まるシェア（３，$g^{F(3)}$）を記述するとともに、当該ユーザＩＤ＝x_iについてシェア（x_i，$g^{F(x_i)}$）を求めるもととなる情報を記述する。

【０１６９】

ユーザＩＤ＝１，２，３以外のユーザＩＤについては、当該ユーザＩＤ＝x_iに対応するシェア（x_i，$g^{F(x_i)}$）を求めることによって、必要な４つのシェアが揃うので、正しいセッション鍵を取得することができる。

【０１７０】

これに対して、無効化対象ユーザＩＤ＝１については、当該ユーザＩＤ＝１に対応するシェア（１，$g^{F(1)}$）を求めても、ヘッダ情報内に記述されているシェアと重複するので、必要な４つのデータが揃わないことになり、正しいセッション鍵を取得することができない。ユーザＩＤ＝２，３についても同様である。

【０１７１】

次に、図１７（ｂ）のように無効化対象ユーザＩＤ＝１～２０が全て同一サブグループU_1に属する場合には、全無効化対象ユーザ数分のシェアを使用するのではなく、前述の第１の実施形態と同様にして、当該１つのサブグループU_1全体を無効化する。すなわち、例えば、１つのサブグループU_1全体を無効化する場合には、当該サブグループU_1についてのみ、正しいセッション鍵が得られないように、（当該サブグループU_1に対応する）セッション鍵を計算するもととなる情報に、間違った値（乱数等）を記述しておく。

【０１７２】
サブグループU_1に属するユーザＩＤについては、セッション鍵を計算するもととなる情報が間違った値になっているので、正しいセッション鍵を取得することができない。
【０１７３】
また、図１７（ｃ）のようにユーザＩＤ＝１～２０すなわち１つのサブグループU_1全体を無効化するとともに、ユーザＩＤ＝２１，２２，２３を無効化する場合には、図５（ａ）の方法と、図１７（ｂ）の方法を組み合わせて実施する。
【０１７４】
この例の場合、ヘッダ情報には、ユーザＩＤ＝２１について求まるシェア（２１，$g^{F(21)}$）、ユーザＩＤ＝２２について求まるシェア（２２，$g^{F(22)}$）、ユーザＩＤ＝２３について求まるシェア（２３，$g^{F(23)}$）を記述する。また、無効化するサブグループU_1についてのみ、正しいシェアが得られないように、（当該サブグループU_1に対応する）シェアを計算するもととなる情報に、間違った値（乱数等）を記述しておく。それ以外のサブグループについては、正しいシェアが得られるように、（当該サブグループに対応する）シェアを計算するもととなる情報に、正しい値を記述しておく。
【０１７５】
サブグループU_1に属するユーザＩＤ以外で且つユーザＩＤ＝２１，２２，２３以外のユーザＩＤについては、正しいシェアを求めることができ、これによって必要な４つのデータが揃うので、正しいセッション鍵を取得することができる。
【０１７６】
ユーザＩＤ＝２１，２２，２３については、正しいシェアを求めることができても、必要な４つのシェアが揃わないので、正しいセッション鍵を取得することができない。
【０１７７】
サブグループU_1に属するユーザＩＤについては、正しいシェアを計算するもととなる情報が間違った値になっているので、正しい４つのシェアが揃わないことになり、結局、正しいセッション鍵を取得することができない。
【０１７８】
以下、鍵生成フェーズ、暗号化フェーズ、復号フェーズ、追跡フェーズの順に説明する。なお、パラメータなどの定義は、特に断りの無い限り、第１の実施形態と同じものを用いる。
【０１７９】
（鍵生成フェーズ）
ｑを素数とし、ｑはｐ－１を割り切り、かつ、ｑはｎ＋４ｋ－１以上であるとする以外は、第１の実施形態と同じである。
【０１８０】
（暗号化フェーズ）
暗号化フェーズにおける無効化対象ユーザ集合をＥとする。すなわち、Ｅは、コンテンツ提供システムで配信用のヘッダ情報を生成する際に無効化とするユーザの集合である。
【０１８１】
コンテンツ提供側システム１のセッション鍵生成部１３は、セッション鍵のもととなる情報ｓをＺｑからランダムに選択し、セッション鍵g^sを計算する。次に、ヘッダ生成部１５は、以下の処理により、木構造Ｔにおけるノードを選択する。
【０１８２】
U_{v_j}がＥに等しい、または含まれるノードv_jが存在する場合、そのようなノードのうち、選択された各U_{v_j}は、互いに共通要素を持たず、かつ、それらの和集合が式（１８）と等しくなるようにノードを選択する。
【数２０】

$$\cup_{v_j \in \{v \mid v \in N, U_v \subseteq E\}} U_{v_j} \qquad (18)$$

【０１８３】
次に、Uv_i、Uv_jがともにＥに等しくない、かつ含まれない兄弟リーフが存在する場合、そのような兄弟リーフを一組選択する。最後に、以下の条件を満たすその他のノードを選択する。条件は、選択された全てのノードv_jについてUv_jは互いに共通要素を持たず、かつ選択された全てのノードv_jについてUv_jの和集合が全ユーザ集合Ｕに等しいことである。
【０１８４】
上記処理終了後、選択されたノードの数をＪとする。
【０１８５】
ヘッダ生成部１５は、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合（式（１９）で表される）を｛x_1、…、x_w｝とする。
【数２１】

$$E \setminus \cup_{v_j \in \{v | v \in N, U_v \subseteq E\}} U_{v_j} \cdot \qquad (19)$$

【０１８６】
例えば、図１７（ｂ）において、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合はU_1であるから、無効化対象ユーザ集合ＥからU_1取り除いた部分集合は、｛２１，２２，２３｝となる。
【０１８７】
このように、ｗは、個別にセッション鍵を復号不能とするユーザの数を示す。
【０１８８】
次に、ヘッダ生成部１５は、$2k(z-1)+1 \leqq w \leqq 2kz$を満たす整数ｚを探し、ヘッダ情報中のシェアの数ｍを、$m=2k(z+1)-1$と設定する。なお、ｋは、前述同様、最大結託人数を示す。
【０１８９】
上記部分集合が空集合である場合、すなわち、個別にセッション鍵を復号不能とするユーザが存在しない場合、$m=2k-1$、$w=0$と設定する。
【０１９０】
個別にセッション鍵を復号不能とするユーザの数ｗが、上記ｍよりも少ない（$w<m$）ならば、不足分の（ｍ－ｗ）個のシェアを得るために、x_{w+1}、…、x_m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。
【０１９１】
ヘッダ生成部１５は、式（２０）を満たす多項式Ｆ（ｘ）をランダムに生成する。
【数２２】

$$F(x) = \sum_{i=0}^{m} \tau_i x^i \bmod q \qquad (20)$$

$$\tau_0 = s$$

【０１９２】
次に、ヘッダ生成部１５は、乱数r_0、r_1を選択する。ヘッダ生成部１５は、選択されたＪ個のノードをv_0、…、v_{J-1}として、$0 \leqq j \leqq J-1$について、式（２１）により、Hv_0、…、Hv_{J-1}を計算する。

【数２３】

$$H_{v_j} = (h_{v_j}, h'_{v_j}, h_{v_j,0}, \ldots, h_{v_j,m}, \hat{h}_1, \ldots, \hat{h}_m)$$

但し、

$$h_{v_j} = g^r$$

$$h'_{v_j} = g^{\lambda_{v_j} r}$$

$$h_{v_j,i} = \begin{cases} g^{r a_i \bmod 2k} g^{\tau_i} & (y_{v_j} \neq i \bmod 2k) \quad \ldots (21a) \\ g^{c_{v_j} r} g^{\tau_i} & (y_{v_j} = i \bmod 2k, U_{v_j} \notin E) \ldots (21b) \\ g^{\gamma_{v_j,i}} & (y_{v_j} = i \bmod 2k, U_{v_j} \subseteq E) \ldots (21c) \end{cases}$$

$$\hat{h}_i = (x_i, g^{F(x_i)})$$

$$F(x) = \sum_{i=0}^{m} \tau_i x^2 \bmod q$$

$$y_{v_j} = v_j \bmod 2k$$

ここで$\gamma_{v_j,i}$はヘッダ生成部１５にて選択される乱数である。

(21)

【０１９３】

なお、式（２１）のうち、セッション鍵を計算するもととなる情報$h_{v_j,i}$の計算式において、式（２１ａ）は、ノードv_jに属するユーザ集合に、個別にセッション鍵を復号不能とするユーザが存在する場合であり、式（２１ｂ）は、ノードv_jに属するユーザ全員が無効化対象でない場合であり、当該ノードv_jに固有の値c_{v_j}が含まれている。また、式（２１ｃ）は、ノードv_jに属するユーザ全員が無効化対象である場合であり、当該ノードv_jに固有の正しい値c_{v_j}に代えて、これとは異なる乱数γ_{v_j}が含まれている。

以上の繰り返し処理により得られたHv_0、…、Hv_{J-1}をヘッダとする。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側システム１を運営することができる。また、第一の実施形態と同様に、以上の繰り返し処理により得られたHv_0、…、Hv_{J-1}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。さらに、上述したノード選択方法以外にも、種々の方法を用いることができる。

【０１９４】

（復号フェーズ）

部分集合Uv_jに属するユーザx_0を考える。ユーザＩＤ＝x_0のユーザ側システム２は、ヘッダを受信した場合、Hv_jを用いて式（２２）を計算する。

【数２４】

$$g^{F(x_0)} = \prod_{i=0}^{m} h_{v_j,i}^{x_0^i} \Big/ \left(h_{v_j}^{A_{v_j}(x_0)} h'^{B(x_0)}_{v_j} \right)^{\sum_{j=0}^{z} x_0^{2jk}}$$

ここで$z = (m+1)/2k - 1$である。$\prod_{i=0}^{m} h_{v_j,i}^{x_0^i}$は以下のように計算される。

$$\prod_{i=0}^{m} h_{v_j,i}^{x_0^i}$$

$$= \prod_{i=0}^{z} \left(h_{v_j,2ik} \times h_{v_j,2ik+1}^{x_0} \times \ldots \times h_{v_j,2ik+y_{v_j}}^{x_0^{y_{v_j}}} \times \ldots \times h_{v_j,2ik+2k-1}^{x_0^{2k-1}} \right)^{x_0^{2ik}}$$

$$= \prod_{l=0}^{z} \left(g^{r\sum_{i=0}^{2k-1} av_{j,i} x_0^i} \right)^{x_0^{2kl}} \times g^{\sum_{j=0}^{m} \tau_j x_0^j}$$

$$= \left(h_{v_j}^{A_{v_j}(x_0)} h'^{B(x_0)}_{v_j} \right)^{\sum_{l=0}^{z} x_0^{2kl}} \times g^{F(x_0)} \qquad (22)$$

ここで、計算された$g^{F(x_0)}$は、ユーザx_0のシェアである。ユーザ側システム２は、$g^{F(x_0)}$とヘッダに含まれているｍ個のシェア$\hat{h}_1, \ldots, \hat{h}_m$を用いて式（２３）を計算し、セッション鍵を得る。

【０１９５】

【数２５】

$$g^{F(0)} = \prod_{j=0}^{m} (g^{F(x_j)})^{\mu_j}$$

$$= g^{\sum_{j=0}^{m} \mu_j F(x_j)}$$

但し、

$$\mu_j = \prod_{0 \le l \le m, l \ne j} \frac{x_l}{x_l - x_j} \bmod q$$

(23)

【０１９６】

（追跡フェーズ）

追跡アルゴリズムの手順例は、第１の実施形態と同様であり、追跡装置による追跡フェーズの動作は、以下に述べる違いを除き、図９に示されているものと同様である。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。

【０１９７】

制御部３３は、図９のステップＳＴ１３において、u_jがＥ（コンテンツ提供システムの上記暗号化フェーズで実際に無効化対象とすべきユーザの集合）に含まれている場合、C_jにC_{j-1}を代入し、ｊを１だけインクリメントする。$\chi = \{u_1, \cdots, u_j\}$とする検査はスキップしてよい。ステップＳＴ１４において、セッション鍵は$g^{F(x0)} = g^s$であり、ヘッダの作成方法は以下に示す通りである。

【０１９８】

ヘッダ生成部３２は、ノードの選択に際して、以下の条件（１）、（２）をともに満たすノードv_jを選択する。（１）Uv_jからχを除いた集合の要素数が「１」以上「２ｋ－１」以下である、又は、Uv_jとχの積集合が空集合である、又は、Uv_jとχの積集合がUv_jである。（２）Uv_jからχを除いた集合の要素数が「１」以上「２ｋ－１」以下であるノードは、多くとも１個である。ヘッダ生成部３２は、選択した各ノードについて、式（２４）によりHv_jを計算する。

【数２６】

$$H_{v_j}=\left(h_{v_j}, h'_{v_j}, h_{v_j,0}, \ldots, h_{v_j,m}, \hat{h}_1, \ldots, \hat{h}_m\right)$$

$$h_{v_j}=\begin{cases} g^{r_0} & (r = r_0) \\ g^{r_1} & (r = r_1) \end{cases}$$

$$h'_{v_j} = \begin{cases} g^{\lambda_{v_j} r_0} & (r = r_0) \\ g^{\lambda_{v_j} r_1} & (r = r_1) \end{cases}$$

$$\hat{h}_i = \left(x_i, g^{F(x_i)}\right)$$

$$F(x) = \sum_{i=0}^{m} \tau_i x^i \bmod q$$

$$y_{v_j}=v_j \bmod 2k$$

(24)

【０１９９】

残りの要素$h_{v_j,i}$については、以下のように計算される。

【０２００】

Uv_jとχの積集合が空集合である場合、式（２５）により計算する。

【数２７】

$$h_{v_j,i} = \begin{cases} g^{r a_i \bmod 2k} g^{\tau_i} & (y_{v_j} \neq i \bmod 2k) \\ g^{c_{v_j} r} g^{\tau_i} & (y_{v_j} = i \bmod 2k, U_{v_j} \notin E) \\ g^{\gamma_{v_j,i}} & (y_{v_j} = i \bmod 2k, U_{v_j} \subseteq E) \end{cases}$$

ここで$\gamma_{v_j,i}$は乱数である。

(25)

【０２０１】

なお、（１）Uv_jからχを除いた集合の要素数が「１」以上「２ｋ－１」以下である、又は、（２）Uv_jとχの積集合がUv_jであり、かつ、Uv_jと、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合が空集合である場合、ｒにr_0を代入する。そうでない場合、ｒにr_0又はr_1をランダムに代入する。

【０２０２】

Uv_jからχを除いた集合の要素数が「１」以上「２ｋ－１」以下である場合、Uv_jからχを除いた集合と、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との和集合を｛x_1、…、x_w｝とする。ｗ＜ｍな

らば、x_{w+1}、…、x_m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。１≦ｔ≦ｍについて、式（２６）を満たすＺｑの要素L_0、…、L_mを求める。

【数２８】

$$\sum_{i=0}^{m} L_i x_t^i = 0 \bmod q \qquad (26)$$

【０２０３】

次に、ｒにｒ$_1$を代入し、式（２７）により$h_{vj,i}$を計算する。

【数２９】

$$h_{v_j,i} = \begin{cases} g^{r_1 a_i \bmod 2k} g^{\tau_i} g^{L_i} & (y_{v_j} \neq i \bmod 2k) \\ g^{c_{v_j} r_1} g^{\tau_i} g^{L_i} & (y_{v_j} = i \bmod 2k) \end{cases} \qquad (27)$$

【０２０４】

Uv_jとχの積集合がUv_jである場合、まず、Uv_jと、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合を計算する。

【０２０５】

Uv_jと、Uv_jがＥに等しい、又は含まれる全てのUv_jとの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合が空集合でない場合、ｒにｒ$_1$を代入し、選択されたノードの内、Uv_iからχを除いた集合の要素数が「１」以上「２ｋ－１」以下であるノードv_iが存在するか否かを判定する。

【０２０６】

選択されたノードの内、Uv_iからχを除いた集合の要素数が「１」以上「２ｋ－１」以下であるノードv_iが存在する場合、式（２８）により$h_{vj,i}$を計算する。

【数３０】

$$h_{v_j,i} = \begin{cases} g^{r_1 a_i \bmod 2k} g^{\tau_i} g^{L_i} & (y_{v_j} \neq i \bmod 2k) \\ g^{c_{v_j} r_1} g^{\tau_i} g^{L_i} & (y_{v_j} = i \bmod 2k) \end{cases} \qquad (28)$$

【０２０７】

選択されたノードの内、Uv_iからχを除いた集合の要素数が「１」以上「２ｋ－１」以下であるノードv_iが存在しない場合、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合を｛x_1、…、x_w｝とする。ｗ＜ｍならば、x_{w+1}、…、x_m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。１≦ｔ≦ｍについて、式（２６）を満たすＺｑの要素L_0、…、L_mを求める。

【０２０８】

次に、式（２９）により$h_{vj,i}$を計算する。

【数３１】

$$h_{v_j,i} = \begin{cases} g^{r_1 a_i \bmod 2k} g^{\tau_i} g^{L_i} & (y_{v_j} \neq i \bmod 2k) \\ g^{c_{v_j} r_1} g^{\tau_i} g^{L_i} & (y_{v_j} = i \bmod 2k) \end{cases} \qquad (29)$$

【０２０９】
なお、L_0、…、L_mが既に生成されている場合は、既に生成されたL_0、…、L_mを用い、新たに生成し直すことはしない。
【０２１０】
Uv_jと、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合が空集合である場合、ｒにr_0又はr_1をランダムに代入し、選択されたノードの内、（１）Uv_iからχを除いた集合の要素数が「１」以上「２ｋ－１」以下である、又は、（２）Uv_iとχの積集合がUv_iであり、かつ、Uv_iと、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合が空集合であるノードv_iが存在するか否かを判定する。
【０２１１】
選択されたノードの内、（１）Uv_iからχを除いた集合の要素数が「１」以上「２ｋ－１」以下である、又は、（２）Uv_iとχの積集合がUv_iであり、かつ、Uv_iと、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合が空集合であるノードv_iが存在する場合、式（３０）により$h_{v_j,i}$を計算する。
【数３２】

$$h_{v_j,i} = \begin{cases} g^{r_0 a_i \bmod 2k} g^{\tau_i} & (y_{v_j} \neq i \bmod 2k,\ r = r_0) \\ g^{r_1 a_i \bmod 2k} g^{\tau_i} g^{L_i} & (y_{v_j} \neq i \bmod 2k,\ r = r_1) \\ g^{\gamma_{v_j,i}} & (y_{v_j} = i \bmod 2k) \end{cases}$$

ここで$\gamma_{v_j,i}$は乱数である。

(30)

【０２１２】
選択されたノードの内、（１）Uv_iからχを除いた集合の要素数が「１」以上「２ｋ－１」以下である、又は、（２）Uv_iとχの積集合がUv_iであり、かつ、Uv_iと、Uv_jがＥに等しい、又は含まれる全てのUv_jの和集合を、無効化対象ユーザ集合Ｅから取り除いた部分集合との積集合が空集合であるノードv_iが存在しない場合、式（３１）により$h_{v_j,i}$を計算する。
【数３３】

$$h_{v_j,i} = \begin{cases} g^{r a_i \bmod 2k} g^{\tau_i} & (y_{v_j} \neq i \bmod 2k) \\ g^{\gamma_{v_j,i}} & (y_{v_j} = i \bmod 2k) \end{cases}$$

(31)

ここで$\gamma_{v_j,i}$は乱数である。

【０２１３】
選択されたノードの数をv_0、…、v_{J-1}とすると、以上の繰り返し処理により得られたHv_0、…、Hv_{J-1}をヘッダとする。
【０２１４】
上述したように第３の実施形態によれば、第１の実施形態と特許文献２において開示された復号鍵無効化方法を組み合わせた構成により、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、有効化対象ユーザ数が第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対応でき、さらに、有効化対象ユーザ数が第１の実施形態の説明において述べた制限を大きく超えた場合の送信オーバヘッドの増加を第２の実施形態に比べてより抑えることができる。また、第１の実施形態と特許文献２において開示された復号鍵無効化方法を組み合わせた構成としても、第１の実施形態と同様の効果を得ることができる。

【０２１５】

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。

【０２１６】

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。

【０２１７】

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。

【０２１８】

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。

【０２１９】

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。

【０２２０】

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。

【０２２１】

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。

【０２２２】

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。

【０２２３】

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。

【０２２４】

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。

【０２２５】

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】

【０２２６】

【図１】本発明の第１の実施形態に係るコンテンツ提供側システム及びユーザ側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】木構造上のルート・ノード・リーフへの、個別鍵生成多項式及び共有鍵生成多項式を割り当てを説明するための図。

【図１４】暗号化フェーズの他の動作を説明するためのフローチャート。

【図１５】木構造を説明するための図。

【図１６】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１７】無効化対象ユーザについて説明するための図。

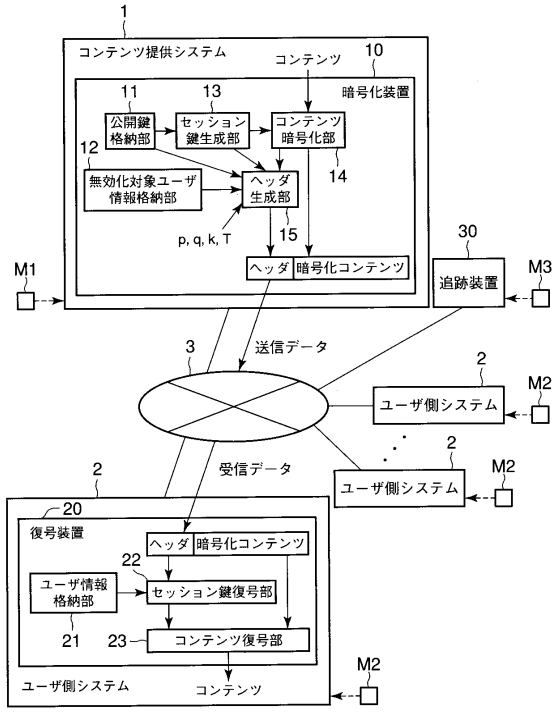
【符号の説明】

【０２２７】

１…コンテンツ提供側システム、２…ユーザ側システム、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。

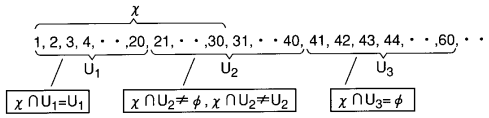
【図１】

図１



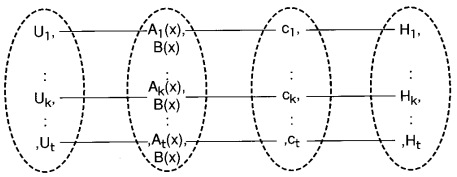
【図２】

図２



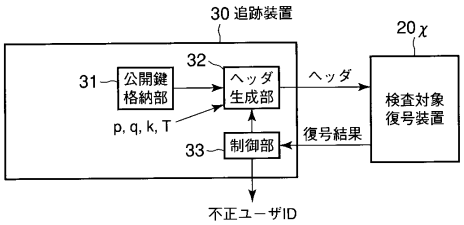
【図３】

図３



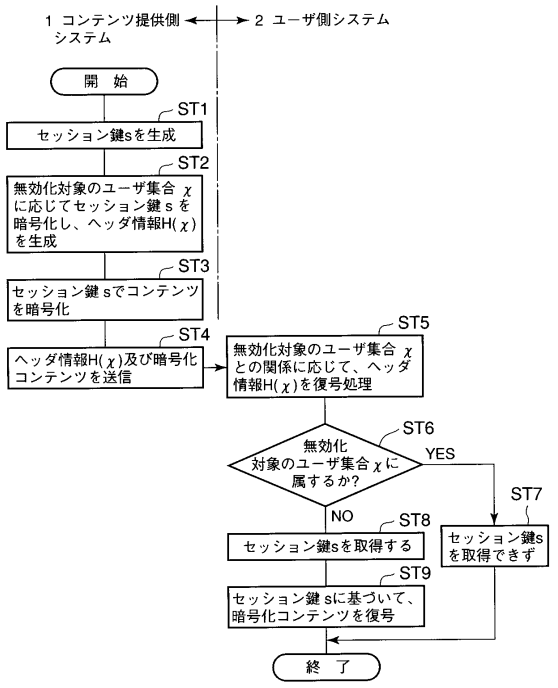
【図４】

図４



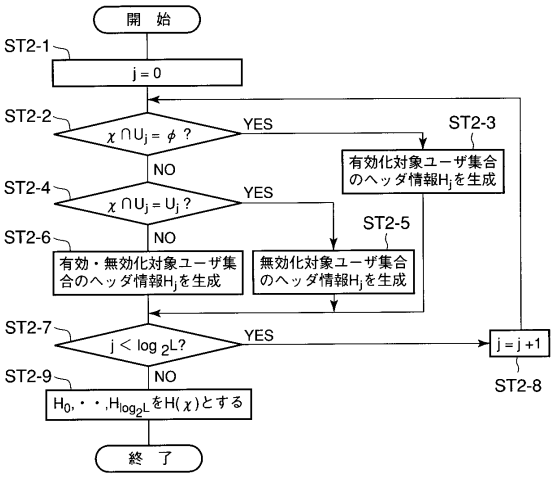
【図５】

図５



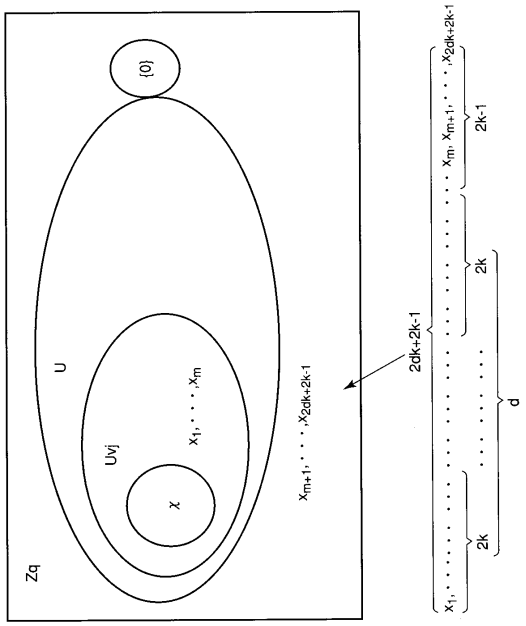
【図６】

図６



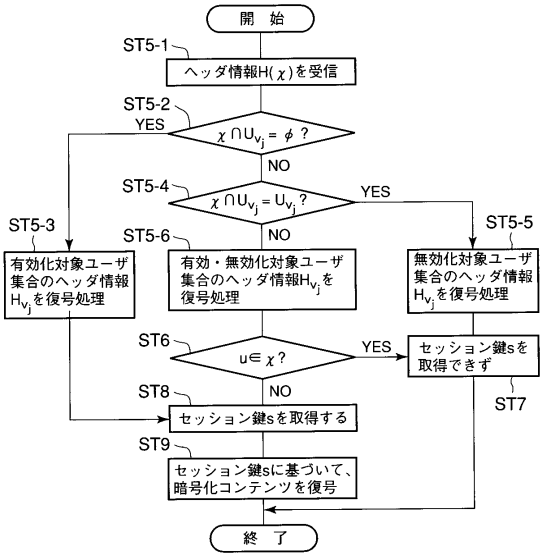
【図７】

図7



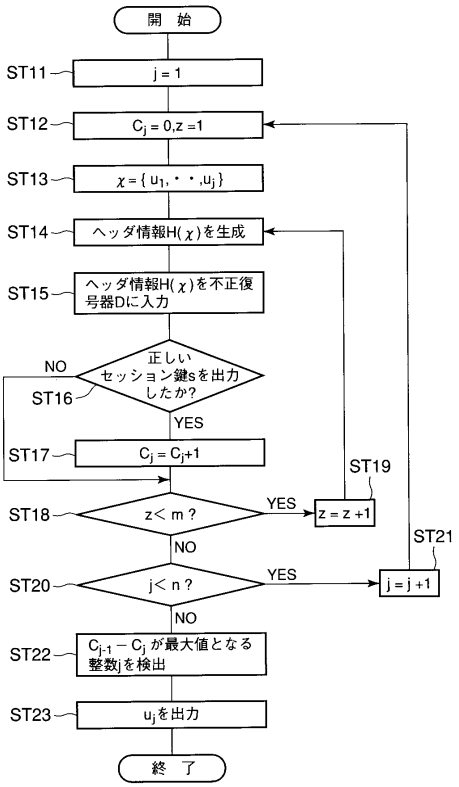
【図８】

図8



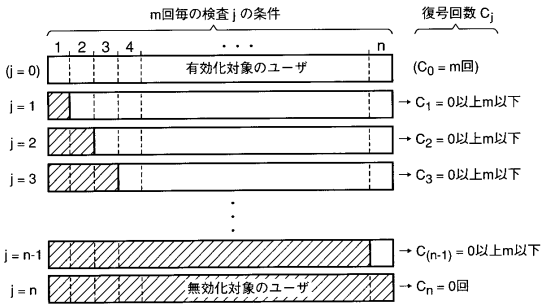
【図９】

図9



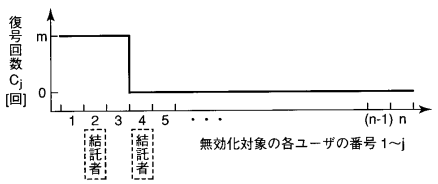
【図１０】

図10



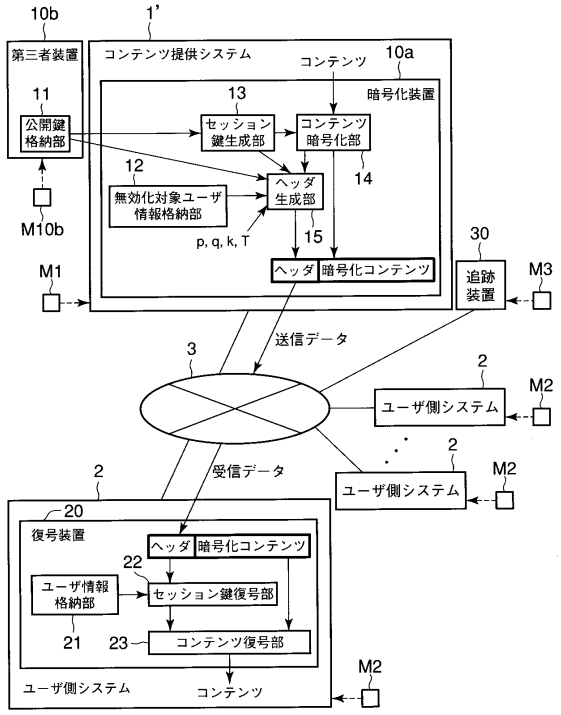
【図１１】

図11



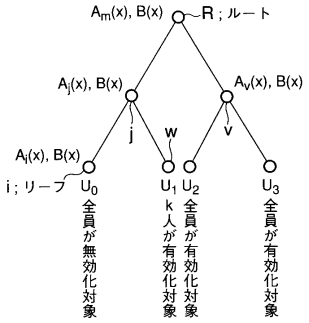
【図１２】

図 12



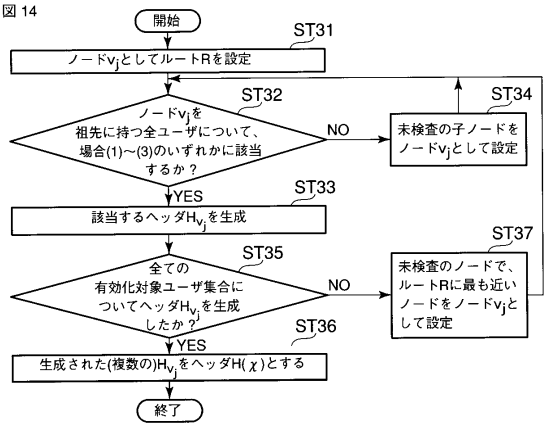
【図１３】

図 13



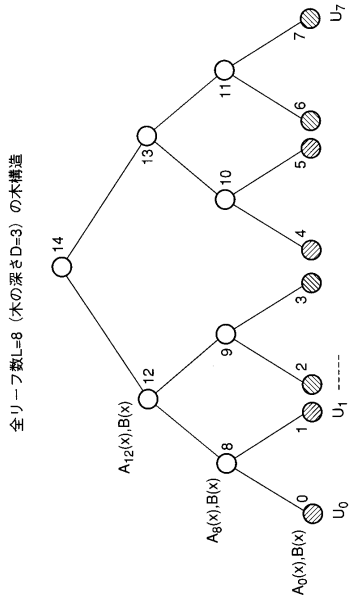
【図１４】

図 14



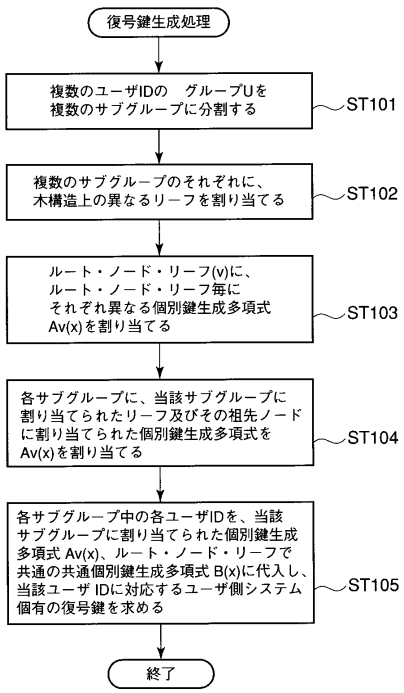
【図１５】

図 15



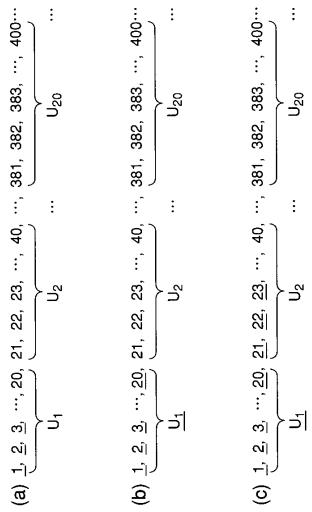
【図１６】

図 16



【図１７】

図17


(a) 1, 2, 3, ..., 20, 21, 22, 23, ..., 40, ..., 381, 382, 383, ..., 400...
U1
U2
U20
...
(b) 1, 2, 3, ..., 20, 21, 22, 23, ..., 40, ..., 381, 382, 383, ..., 400...
U1
U2
U20
...
(c) 1, 2, 3, ..., 20, 21, 22, 23, ..., 40, ..., 381, 382, 383, ..., 400...
U1
U2
U20
...

フロントページの続き

(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 松下 達之
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内

審査官 青木 重徳

(56)参考文献 特開２００３－２８９２９６（ＪＰ，Ａ）
特開２００３－０８７２３２（ＪＰ，Ａ）
特開２００２－３１４５３２（ＪＰ，Ａ）
特開２００２－１５２１８７（ＪＰ，Ａ）
MoonShik Lee, Daegun Ma, and MinJae Seo, “Breaking Two k-Resilient Traitor Tracing Schemes with Sublinear Ciphertext Size”, LNCS, ２００９年 6月, Vol.5536, p.238-252, Applied Cryptogoraphy and Network Security
Tatsuyuki Matsushita and Hideki Imai, “Hierarchical Key Assignment for Black-Box Tracing with Efficient Ciphertext Size”, LNCS, ２００６年１２月, Vol.4307, p.92-111, Information and Communications Security
松下達之，今井秀樹，“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”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００６年 7月１４日，Ｖｏｌ．１０６，Ｎｏ．１７６，ｐ．９１－９８，ＩＳＥＣ２００６－４０～７１，情報セキュリティ
花岡悟一郎，小川一人，藤井亜里砂，大竹剛，真島恵吾，小山田公之，今井秀樹，“トレードオフ不正利用者追跡法”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００４年 9月１０日，Ｖｏｌ．１０４，Ｎｏ．３１５，ｐ．３９－４５，ＩＳＥＣ２００４－６７～７７
小川一人，藤井亜里砂，大竹剛，花岡悟一郎，真島恵吾，小山田公之，今井秀樹，“鍵漏洩耐性を持つ不正者追跡法”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００４年 7月１３日，Ｖｏｌ．１０４，Ｎｏ．１９９，ｐ．１５１－１５８，ＩＳＥＣ２００４－１３～４０，情報セキュリティ
松下達之，今井秀樹，“より強力な攻撃者に対するブラックボックス追跡”，２００４年暗号と情報セキュリティシンポジウム予稿集ＣＤ－ＲＯＭ，日本，２００４年 1月２７日，１Ｃ５ディジタルコンテンツ保護II，１Ｃ５－５

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８