【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成23年1月6日(2011.1.6)

【公開番号】特開2006-60793(P2006-60793A)
【公開日】平成18年3月2日(2006.3.2)
【年通号数】公開・登録公報2006-009
【出願番号】特願2005-210645(P2005-210645)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/24　(2006.01)
Ｇ０６Ｆ　21/06　(2006.01)
Ｈ０４Ｎ　7/16　(2011.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　12/14　５４０Ｂ
Ｇ０６Ｆ　12/14　５４０Ｐ
Ｇ０６Ｆ　12/14　５６０Ｅ
Ｈ０４Ｎ　7/16　Ｚ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成22年11月15日(2010.11.15)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報を送受信する方法であって、
前記コンテンツ利用情報の送信元装置が前記コンテンツ利用情報の送信先装置を認証するステップと、
前記送信先装置が承認された場合に、前記送信元装置と前記送信先装置の間で第１の対称鍵を共有するステップと、
前記送信元装置が、前記コンテンツ利用情報を暗号化して前記送信先装置へ送信するステップと、を含み、
前記第１の対称鍵を共有するステップは、
Elliptic Curve Diffie-Hellman暗号アルゴリズムにより、前記送信先装置の公開鍵を用いて、前記第１の対称鍵を前記送信先装置との間で共有するためのデータを生成するステップと、
前記データを相手の装置に送信するステップと、を含み、
前記コンテンツ利用情報を送信するステップは、
前記コンテンツ利用情報を送信するタイミングが到来したときに、前記送信元装置と前記送信先装置の間で第２の対称鍵を共有するステップと、
前記第１の対称鍵及び前記第２の対称鍵により前記コンテンツ利用情報を暗号化して前記送信先装置へ送信するステップと、を含む
ことを特徴とするコンテンツ利用情報送信方法。
【請求項２】

前記第１の対称鍵は、前記コンテンツ利用情報を送信するステップの終了後も、前記送信元装置及び前記送信先装置において保持されて、次にコンテンツ利用情報を送信するときに利用されることを特徴とする請求項１に記載のコンテンツ利用情報送信方法。
【請求項３】
前記第２の対称鍵は、前記コンテンツ利用情報を送受信するステップの終了後に、次のコンテンツ利用情報を送信するときには新たに発行され、前記送信元装置及び前記送信先装置の間で共有されることを特徴とする請求項１又は２に記載のコンテンツ利用情報送信方法。
【請求項４】
前記第１の対称鍵は、前記送信元装置及び前記送信先装置のうちいずれか一方が発行し、前記第２の対称鍵は、他方が発行することを特徴とする請求項１から３のいずれかに記載のコンテンツ利用情報送信方法。
【請求項５】
前記第２の対称鍵を共有するために使用する第３の対称鍵を前記送信元装置と前記送信先装置との間で共有するステップを更に含み、
前記第２の対称鍵を共有するステップは、前記第２の対称鍵を前記第３の対称鍵で暗号化して送受信することにより前記第２の対称鍵を共有することを特徴とする請求項１から４のいずれかに記載のコンテンツ利用情報送信方法。
【請求項６】
前記第３の対称鍵は、前記コンテンツ利用情報を送信するステップの終了後も、前記送信元装置及び前記送信先装置において保持されて、次に前記第２の対称鍵を共有するときに利用されることを特徴とする請求項５に記載のコンテンツ利用情報送信方法。
【請求項７】
前記送信元装置及び前記送信先装置の一方は、ストレージデバイスであることを特徴とする請求項１から６のいずれかに記載のコンテンツ利用情報送信方法。
【請求項８】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、
前記コンテンツ利用情報享受装置から認証情報を取得して、その認証情報の正当性を検証する検証手段と、
前記検証手段が前記コンテンツ利用情報享受装置を承認したときに、前記コンテンツ利用情報享受装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、
前記コンテンツ利用情報を送信するタイミングが到来したときに、前記コンテンツ利用情報享受装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、
前記コンテンツ利用情報を前記第１の対称鍵及び前記第２の対称鍵により暗号化する暗号化手段と、
前記暗号化手段により暗号化された前記コンテンツ利用情報を前記コンテンツ利用情報享受装置へ送信するコンテンツ利用情報送信手段と、を備え、
前記第１の対称鍵共有手段は、
乱数を発生する乱数発生手段と、
Elliptic Curve Diffie-Hellman暗号アルゴリズムにより前記乱数と前記コンテンツ利用情報享受装置の公開鍵を用いて前記第１の対称鍵を生成するとともに、前記第１の対称鍵を前記コンテンツ利用情報享受装置との間で共有するためのデータを生成する第１の対称鍵生成手段と、
前記データを前記コンテンツ利用情報享受装置に送信する送信手段と、を含む
ことを特徴とするコンテンツ利用情報提供装置。
【請求項９】
前記コンテンツ利用情報提供装置は、
前記コンテンツ利用情報を生成するコンテンツ利用情報生成部と、

前記コンテンツデータを前記コンテンツ鍵によって暗号化し、前記暗号化コンテンツデータを出力するコンテンツデータ暗号部と、
を更に備えることを特徴とする請求項８に記載のコンテンツ利用情報提供装置。
【請求項１０】
前記コンテンツ利用情報提供装置は、
前記暗号化コンテンツデータを格納する第１の格納部と、
前記コンテンツ利用情報を格納する第２の格納部と、を更に備え、
前記第２の格納部は、耐タンパ構造によって構成されることを特徴とする請求項８又は９に記載のコンテンツ利用情報提供装置。
【請求項１１】
暗号化されたコンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報享受装置に提供するコンテンツ利用情報提供装置であって、
前記コンテンツ利用情報享受装置との間でデータの授受を制御するインタフェースと、
前記コンテンツ利用情報享受装置との通信においてテンポラルに生成する第１の対称鍵を生成する対称鍵生成部と、
前記コンテンツ利用情報享受装置に設定された第１の公開鍵によって、データを暗号化する第１の暗号部と、
前記対称鍵生成部により生成された第１対称鍵によってデータを復号する復号部と、
前記コンテンツ利用情報享受装置に設定された楕円曲線暗号の第２の公開鍵を用いて、Ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ　Ｄｉｆｆｉｅ　－　Ｈｅｌｌｍａｎ暗号アルゴリズムにしたがい、データを暗号化する第２の暗号部と、
前記第２の暗号部に供給する乱数を生成する乱数生成部と、
前記コンテンツ利用情報享受装置で生成された第２の対称鍵によってデータを暗号化する第３の暗号部と、
制御部とを備え、
前記第２の暗号部は、
前記乱数生成部において生成された乱数を取得し、前記取得した乱数と前記第２の公開鍵に基づいて、暗号化に用いるシェアード鍵と、このシェアード鍵を前記コンテンツ利用情報享受装置と共有するためのデータとを生成する機能と、前記生成したシェアード鍵によって前記コンテンツ利用情報を暗号化する機能を有し、
前記対称鍵生成部において前記第１の対称鍵が生成されて初めての前記第２の公開鍵による暗号化処理において、前記乱数生成部において生成された乱数を取得し、前記取得した乱数と前記第２の公開鍵に基づいて、暗号化に用いるシェアード鍵と、このシェアード鍵を前記コンテンツ利用情報享受装置と共有するためのデータとを生成し、前記シェアード鍵によってデータを暗号化し、
前記対称鍵生成部において前記第１の対称鍵が生成されて２回目以降の暗号化処理において、前回のシェアード鍵によって前記コンテンツ利用情報を暗号化し、
前記制御部は、
前記第１の対称鍵を生成するように前記対称鍵生成部を制御し、
前記第１の公開鍵によって暗号化された前記第１の対称鍵を前記第１の暗号部から受け取って、前記インタフェースを介して前記コンテンツ利用情報享受装置へ送信し、
前記インタフェースを介して受信した前記第１の対称鍵によって暗号化された前記第２の対称鍵および前記第２の公開鍵を、前記コンテンツ利用情報享受装置から受け取って前記復号部に与え、
前記復号部で復号した第２の公開鍵に基づいて生成されたシェアード鍵と第２の対称鍵とによって暗号化された暗号化コンテンツ利用情報を前記第２の暗号部または前記第３の暗号部から受け取って、前記インタフェースを介して前記コンテンツ利用情報享受装置へ送信する
ことを特徴とするコンテンツ利用情報提供装置。
【請求項１２】

前記コンテンツ利用情報を生成し、かつ、生成したコンテンツ利用情報に含まれる前記コンテンツ鍵でコンテンツデータを暗号化するコンテンツ暗号部をさらに備え、
前記制御部は、前記コンテンツ暗号部が生成した前記コンテンツ利用情報を取得し、前記第３の暗号部に与える、請求項１１に記載のコンテンツ利用情報提供装置。
【請求項１３】
本コンテンツ利用情報提供装置は、ストレージデバイスであることを特徴とする請求項８から１２のいずれかに記載のコンテンツ利用情報提供装置。
【請求項１４】
暗号化コンテンツデータを復号するためのコンテンツ鍵を含むコンテンツ利用情報をコンテンツ利用情報提供装置から享受するコンテンツ利用情報享受装置であって、
前記コンテンツ利用情報提供装置に自身の認証情報を送信する認証情報送信手段と、
前記コンテンツ利用情報提供装置が前記認証情報を承認したときに、前記コンテンツ利用情報提供装置との間で公開鍵暗号方式を用いて第１の対称鍵を共有する第１の対称鍵共有手段と、
前記コンテンツ利用情報を受信するタイミングが到来したときに、前記コンテンツ利用情報提供装置との間で第２の対称鍵を共有する第２の対称鍵共有手段と、
前記第１の対称鍵及び前記第２の対称鍵により暗号化された前記コンテンツ利用情報を前記コンテンツ利用情報提供装置から受信するコンテンツ利用情報受信手段と、
前記暗号化された前記コンテンツ利用情報を復号する復号手段と、を備え、
前記第１の対称鍵共有手段は、
前記コンテンツ利用情報提供装置に自身の公開鍵を提供する公開鍵提供手段と、
前記第１の対称鍵を前記コンテンツ利用情報提供装置との間で共有するためのデータを取得する取得手段と、
Elliptic Curve Diffie-Hellman暗号アルゴリズムにより前記データと前記公開鍵と対をなす秘密鍵とを用いて前記第１の対称鍵を生成する第１の対称鍵生成手段と、を含むことを特徴とするコンテンツ利用情報享受装置。
【請求項１５】
前記コンテンツ利用情報享受装置は、
前記暗号化コンテンツデータを前記コンテンツ鍵により復号するコンテンツデータ復号部と、
前記コンテンツデータ復号部により復号されたコンテンツデータを再生する再生部と、
を更に備えることを特徴とする請求項１４に記載のコンテンツ利用情報享受装置。
【請求項１６】
前記コンテンツ利用情報享受装置は、
前記暗号化コンテンツデータを格納する第１の格納部と、
前記コンテンツ利用情報を格納する第２の格納部とを含み、
前記第２の格納部は、耐タンパ構造によって構成されることを特徴とする請求項１４又は１５に記載のコンテンツ利用情報享受装置。
【請求項１７】
本コンテンツ利用情報享受装置は、ストレージデバイスであることを特徴とする請求項１４から１６のいずれかに記載のコンテンツ利用情報享受装置。