【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19年9月27日(2007.9.27)

【公開番号】特開2006-74392(P2006-74392A)
【公開日】平成18年3月16日(2006.3.16)
【年通号数】公開・登録公報2006-011
【出願番号】特願2004-254681(P2004-254681)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成19年8月10日(2007.8.10)
【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】
所定軸に沿って並んだ部分コンテンツで構成されるコンテンツ情報を暗号化する情報暗号化装置であって、
前記コンテンツ情報のルート鍵情報を生成するルート鍵生成手段と、
第i層のi個の鍵を、上位の第i-1層のi-1個の鍵に基づき生成し、末端位置に前記部分コンテンツの数分の鍵情報を生成する生成する階層鍵生成手段と、
ここで、当該階層鍵生成手段は、第ｉ層のｊ番目のノード鍵をＰ(i,j)(j=1,2,…,i)と表現した場合、両端のノード鍵Ｐ(i,1)及びＰ(i,i)については、上位の第i-1層のノード鍵Ｐ(i-1,1),Ｐ(i-1,i-1)から一方向関数に従って生成し、ノード鍵Ｐ(i,m)(m=2,3,…,i-1）については、上位の第i-1層中のノード鍵Ｐ(i-1,m-1),Ｐ(i-1,m）のいずれからも生成可能な一方向関数で生成する；
前記階層鍵生成手段で生成された末端層の鍵情報を用いて、各部分コンテンツを暗号化する暗号化手段と、
該暗号化手段で暗号化した部分コンテンツで構成される暗号化済みのコンテンツ情報と、前記ルート鍵情報、並びに、各部分コンテンツの区切り位置を特定する情報を記憶する記憶手段と
を備えることを特徴とする情報暗号化装置。
【請求項２】
前記ルート鍵生成手段は、前記部分コンテンツの数に応じた個数のデータを入力する入力手段を含み、当該入力手段で入力されたデータに基づいてルート鍵情報を生成することを特徴とする請求項１に記載の情報暗号化装置。
【請求項３】
更に、前記コンテンツ情報から、各部分コンテンツの区切り位置を指定する指定手段とを備えることを特徴とする請求項１に記載の情報暗号化装置。
【請求項４】
前記コンテンツ情報は、動画情報、音響情報、文書情報を含むことを特徴とする請求項１乃至３のいずれか１項に記載の情報暗号化装置。
【請求項５】

更に、コンテンツ情報の区切り位置を指定する指定手段を備え、
前記部分コンテンツは、前記指定手段で指定された区切り位置間、或いは前記コンテンツの端部と最寄りの区切り位置間で決定されることを特徴とする請求項１に記載の情報暗号化装置。
【請求項６】
請求項１に記載の情報暗号化装置で暗号化されたコンテンツを復号するための鍵情報を配信する情報配信装置であって、
復号する部分コンテンツの範囲を決定する決定手段と、
前記記憶手段で記憶されたルート鍵情報に基づき、復号用の鍵情報を階層化して生成する第２の階層鍵生成手段と、
ここで、第２の階層鍵生成手段は、第ｉ層のｊ番目のノード鍵をＰ(i,j)(j=1,2,…,i）と表現した場合、両端のノード鍵Ｐ(i,1)及びＰ(i,i)については、上位の第i-1層のノード鍵Ｐ(i-1,1),Ｐ(i-1,i-1)から一方向関数に従って生成し、ノード鍵Ｐ(i,m)(m=2,3,…,i-1）については、上位の第i-1層中のノード鍵Ｐ(i-1,m-1),Ｐ(i-1,m）のいずれからも生成可能な一方向関数で生成する；
前記決定手段で決定した部分コンテンツの範囲に対応する末端位置のノードの全てが子ノードとなるノードのうち最下位に位置するノードの鍵情報と、少なくとも前記部分コンテンツの範囲内の各部分コンテンツの区切り位置を示す情報で構成される復号情報を配信する配信手段と
を備えることを特徴とする情報配信装置。
【請求項７】
所定軸に沿って並んだ部分コンテンツで構成されるコンテンツ情報を暗号化する情報暗号化装置の制御方法であって、
前記コンテンツ情報のルート鍵情報を生成するルート鍵生成工程と、
第i層のi個の鍵を、上位の第i-1層のi-1個の鍵に基づき生成し、末端位置に前記部分コンテンツの数分の鍵情報を生成する生成する階層鍵生成工程と、
ここで、階層鍵生成工程は、第ｉ層のｊ番目のノード鍵をＰ(i,j)(j=1,2,…,i）と表現した場合、両端のノード鍵Ｐ(i,1)及びＰ(i,i)については、上位の第i-1層のノード鍵Ｐ(i-1,1),Ｐ(i-1,i-1)から一方向関数に従って生成し、ノード鍵Ｐ(i,m)(m=2,3,…,i-1）については、上位の第i-1層中のノード鍵Ｐ(i-1,m-1),Ｐ(i-1,m）のいずれからも生成可能な一方向関数で生成する；
前記階層鍵生成工程で生成された末端層の鍵情報を用いて、各部分コンテンツを暗号化する暗号化工程と、
該暗号化工程で暗号化した部分コンテンツで構成される暗号化済みのコンテンツ情報と、前記ルート鍵情報、並びに、各部分コンテンツの区切り位置を特定する情報を所定の記憶手段に格納する格納工程と
を備えることを特徴とする情報暗号化装置の制御方法。
【請求項８】
請求項１に記載の情報暗号化装置で暗号化されたコンテンツを復号するための鍵情報を配信する情報配信装置の制御方法であって、
復号する部分コンテンツの範囲を決定する決定工程と、
前記記憶手段で記憶されたルート鍵情報に基づき、復号用の鍵情報を階層化して生成する第２の階層鍵生成工程と、
ここで、第ｉ層のｊ番目のノード鍵をＰ(i,j)(j=1,2,…,i）と表現した場合、両端のノード鍵Ｐ(i,1)及びＰ(i,i)については、上位の第i-1層のノード鍵Ｐ(i-1,1),Ｐ(i-1,i-1)から一方向関数に従って生成し、ノード鍵Ｐ(i,m)(m=2,3,…,i-1）については、上位の第i-1層中のノード鍵Ｐ(i-1,m-1),Ｐ(i-1,m）のいずれからも生成可能な一方向関数で生成する；
前記決定工程で決定した部分コンテンツの範囲に対応する末端位置のノードの全てが子ノードとなるノードのうち最下位に位置するノードの鍵情報と、少なくとも前記部分コン

テンツの範囲内の各部分コンテンツの区切り位置を示す情報で構成される復号情報を配信する配信工程と
を備えることを特徴とする情報配信装置の制御方法。
【請求項９】
コンピュータが読み込み実行することで、前記コンピュータを、所定軸に沿って並んだ部分コンテンツで構成されるコンテンツ情報を暗号化する情報暗号化装置として機能させるコンピュータプログラムであって、
前記コンテンツ情報のルート鍵情報を生成するルート鍵生成手段と、
第i層のi個の鍵を、上位の第i-1層のi-1個の鍵に基づき生成し、末端位置に前記部分コンテンツの数分の鍵情報を生成する生成する階層鍵生成手段と、
ここで、階層鍵生成手段は、第ｉ層のｊ番目のノード鍵をＰ(i,j)(j=1,2,…,i）と表現した場合、両端のノード鍵Ｐ(i,1)及びＰ(i,i)については、上位の第i-1層のノード鍵Ｐ(i-1,1),Ｐ(i-1,i-1)から一方向関数に従って生成し、ノード鍵Ｐ(i,m)(m=2,3,…,i-1）については、上位の第i-1層中のノード鍵Ｐ(i-1,m-1),Ｐ(i-1,m）のいずれからも生成可能な一方向関数で生成する；
前記階層鍵生成手段で生成された末端層の鍵情報を用いて、各部分コンテンツを暗号化する暗号化手段と、
該暗号化手段で暗号化した部分コンテンツで構成される暗号化済みのコンテンツ情報と、前記ルート鍵情報、並びに、各部分コンテンツの区切り位置を特定する情報を記憶する記憶手段
として機能させることを特徴とするコンピュータプログラム。
【請求項１０】
コンピュータが読み込み実行することで、前記コンピュータを、請求項１に記載の情報暗号化装置で暗号化されたコンテンツの復号するための鍵情報を配信する情報配信装置として機能させるコンピュータプログラムであって、
復号する部分コンテンツの範囲を決定する決定手段と、
前記記憶手段で記憶されたルート鍵情報に基づき、復号用の鍵情報を階層化して生成する第２の階層鍵生成手段と、
ここで、第２の階層鍵生成手は、段第ｉ層のｊ番目のノード鍵をＰ(i,j)(j=1,2,…,i）と表現した場合、両端のノード鍵Ｐ(i,1)及びＰ(i,i)については、上位の第i-1層のノード鍵Ｐ(i-1,1),Ｐ(i-1,i-1)から一方向関数に従って生成し、ノード鍵Ｐ(i,m)(m=2,3,…,i-1）については、上位の第i-1層中のノード鍵Ｐ(i-1,m-1),Ｐ(i-1,m）のいずれからも生成可能な一方向関数で生成する；
前記決定手段で決定した部分コンテンツの範囲に対応する末端位置のノードの全てが子ノードとなるノードのうち最下位に位置するノードの鍵情報と、少なくとも前記部分コンテンツの範囲内の各部分コンテンツの区切り位置を示す情報で構成される復号情報を配信する配信手段
として機能させることを特徴とするコンピュータプログラム。
【請求項１１】
請求項９又は１０に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。