

(19) 日本国特許庁 (JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-170066

(P2012-170066A)

(43) 公開日 平成24年9月6日 (2012. 9. 6)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 9/08 (2006.01)	H04L 9/00 601B	5J104
H04L 9/14 (2006.01)	H04L 9/00 641	
G06F 21/24 (2006.01)	G06F 21/24 166A	

審査請求 未請求 請求項の数 15 O L 外国語出願 (全 16 頁)

(21) 出願番号	特願2012-24738 (P2012-24738)	(71) 出願人	501263810
(22) 出願日	平成24年2月8日 (2012. 2. 8)		トムソン ライセンシング
(31) 優先権主張番号	11305134.6		Thomson Licensing
(32) 優先日	平成23年2月10日 (2011. 2. 10)		フランス国, 92130 イッシー レ
(33) 優先権主張国	欧州特許庁 (EP)		ムーリノー, ル ジャンヌ ダルク,
			1-5
			1-5, rue Jeanne d' A
			rc, 92130 ISSY LES
			MOULINEAUX, France
		(74) 代理人	100070150
			弁理士 伊東 忠彦
		(74) 代理人	100091214
			弁理士 大貫 進介
		(74) 代理人	100107766
			弁理士 伊東 忠重

最終頁に続く

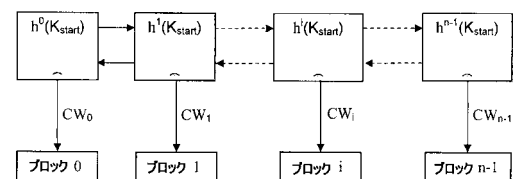
(54) 【発明の名称】 制御語を生成する方法および装置

(57) 【要約】 (修正有)

【課題】 コンテンツ項目の暗号化のためのn個の制御語を生成する。

【解決手段】 装置が第一の鍵 K_{start} および第二の鍵 K_{end} を取得し、n個の制御語を生成する。生成された制御語を使って暗号化されたコンテンツ項目のためのライセンスが生成される。ライセンスは第一の鍵 K_{start} 、第二の鍵 K_{end} および整数nを含み、ライセンスは受信者に送信される。第一の鍵と第二の鍵の間にある第三の鍵および第四の鍵を受信者に送ることができるが、受信者は第三の鍵と第四の鍵の「外側」にある制御語を生成することはできない。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

n を整数として、コンテンツ項目の n 個の連続するユニットの暗号化または復号のための n 個の制御語を生成する装置であって：

第一の鍵 K_{start} および第二の鍵 K_{end} を取得し；

前記第一の鍵 K_{start} に第一の一方向性関数を逐次反復的に適用することによって n 個のサブ鍵 $K1_0 \sim K1_{n-1}$ の第一の順序付き集合を生成するとともに、前記第二の鍵 K_{end} に第二の一方向性関数を逐次反復的に適用することによって n 個のサブ鍵 $K2_0 \sim K2_{n-1}$ の第二の順序付き集合を生成し；

$0 \leq i \leq n-1$ として、 n 個のサブ鍵の前記第一の順序付き集合からのサブ鍵 $K1_i$ および n 個のサブ鍵の前記第二の順序付き集合からのサブ鍵 $K2_{n-i-1}$ から制御語 i を生成する組み合わせ演算を逐次反復的に使うことにより n 個の制御語を生成し；

n 個の生成された制御語を出力するよう構成されたプロセッサを有する、装置。

【請求項 2】

前記第一の一方向性関数および前記第二の一方向性関数の少なくとも一方はハッシュ関数である、請求項 1 記載の装置。

【請求項 3】

前記第一の一方向性関数および前記第二の一方向性関数の少なくとも一方は公開鍵暗号化である、請求項 1 または 2 記載の装置。

【請求項 4】

前記組み合わせ演算はXORである、請求項 1 記載の装置。

【請求項 5】

前記組み合わせ演算は連結または公開鍵暗号化または対称鍵暗号化である、請求項 1 記載の装置。

【請求項 6】

前記プロセッサがさらに、前記コンテンツ項目をそれぞれ複数のユニットを含む複数の部分に分離し、各部分について独立に制御語を生成するよう構成されている、請求項 1 記載の装置。

【請求項 7】

前記プロセッサがさらに、生成された制御語 i を使ってユニット i が暗号化されている前記コンテンツ項目についてのライセンスを生成し、前記ライセンスは前記第一の鍵 K_{start} 、前記第二の鍵 K_{end} および前記整数 n を含み；

前記ライセンスを受信機に送信するよう構成されている、請求項 1 記載の装置。

【請求項 8】

前記コンテンツ項目がより長いコンテンツ項目の抜粋であり、前記より長いコンテンツ項目が第三の鍵および第四の鍵から生成された制御語を使って暗号化されたものであり、前記プロセッサがさらに：

前記第一の鍵 K_{start} を前記第一の一方向性関数の前記第三の鍵への逐次反復的適用によって生成し、

前記第二の鍵 K_{end} を前記第二の一方向性関数の前記第四の鍵への逐次反復的適用によって生成するようさらに構成されている、請求項 7 記載の装置。

【請求項 9】

前記コンテンツ項目が暗号化されており、前記プロセッサがさらに、生成された制御語を使って暗号化されたコンテンツ項目を復号するよう構成されている、請求項 1 記載の装置。

【請求項 10】

コンテンツ項目の n 個の連続するユニットの暗号化または復号のための n 個の制御語を生

10

20

30

40

50

成する方法であって、 n は整数であり、当該方法は、装置において：

- ・ 第一の鍵 K_{start} および第二の鍵 K_{end} を取得する段階と；
- ・ 前記第一の鍵 K_{start} に第一の一方向性関数を逐次反復的に適用することによって n 個のサブ鍵 $K1_0 \sim K1_{n-1}$ の第一の順序付き集合を生成するとともに、前記第二の鍵 K_{end} に第二の一方向性関数を逐次反復的に適用することによって n 個のサブ鍵 $K2_0 \sim K2_{n-1}$ の第二の順序付き集合を生成する段階と；
- ・ $0 \leq i \leq n-1$ として、 n 個のサブ鍵の前記第一の順序付き集合からのサブ鍵 $K1_i$ および n 個のサブ鍵の前記第二の順序付き集合からのサブ鍵 $K2_{n-i-1}$ から制御語 i を生成する組み合わせ演算を逐次反復的に使うことにより n 個の制御語を生成する段階と；
- ・ n 個の生成された制御語を出力する段階とを含む、

10

方法。

【請求項 1 1】

前記第一の一方向性関数および前記第二の一方向性関数の少なくとも一方はハッシュ関数である、請求項 1 0 記載の方法。

【請求項 1 2】

前記組み合わせ演算がXORである、請求項 1 0 記載の方法。

【請求項 1 3】

前記コンテンツ項目をそれぞれ複数のユニットを含む複数の部分に分離する段階をさらに含み、請求項 1 0 記載の各段階が各部分について独立に実行される、請求項 1 記載の方法。

20

【請求項 1 4】

請求項 1 0 記載の方法によって生成された制御語を使って暗号化されているコンテンツ項目についてのコンテンツ・ライセンスを生成する方法であって、装置において：

- ・ 生成された制御語 i を使ってユニット i が暗号化されている前記コンテンツ項目についてのライセンスを生成する段階であって、前記ライセンスは前記第一の鍵 K_{start} 、前記第二の鍵 K_{end} および前記整数 n を含む、段階と；
- ・ 前記ライセンスを受信機に送信する段階とを含む、

方法。

【請求項 1 5】

請求項 1 4 記載の方法であって、前記コンテンツ項目がより長いコンテンツ項目の抜粋であり、前記より長いコンテンツ項目は第三の鍵および第四の鍵から生成された制御語を使って暗号化されたものであり、当該方法がさらに：

30

- ・ 前記第一の鍵 K_{start} を前記第一の一方向性関数の前記第三の鍵への逐次反復的適用によって生成する段階と；
- ・ 前記第二の鍵 K_{end} を前記第二の一方向性関数の前記第四の鍵への逐次反復的適用によって生成する段階をさらに含む、

方法。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

40

本発明は概括的にはデジタル著作権管理（DRM: Digital Rights Management）に、より詳細にはDRM保護されたデジタル・コンテンツについての制御語の生成に関する。

【背景技術】

【0 0 0 2】

この節は、読者に技術の諸側面を紹介するために意図されている。それらの側面は、下記に記載および／または特許請求される本発明のさまざまな側面に関係することがありうる。この議論は、読者に、本発明のさまざまな側面のよりよい理解を容易にする背景情報を与える助けになると思われる。よって、これらの陳述はこの観点で読まれるべきであって、従来技術の自認として読まれるべきではないことを理解しておくべきである。

【0 0 0 3】

50

DRMソリューションはしばしばユーザー・フレンドリーでないと考えられる。よくある不満は、DRMが1998年のデジタル・ミレニアム著作権法（非特許文献1）によって規定されるフェアユースを禁止するというものである。フェアユースの一部であると考えられる多くのことのうちには、エンドユーザーが作品、すなわちコンテンツ項目の抜粋を、批評、学究などのために引用または使用する権利がある。しかしながら、従来技術のDRMソリューションではこれは可能ではない。

【0004】

よって、次のことができるDRMソリューションが必要とされている：

- ・不法または無許諾の使用がされないようコンテンツ項目を保護する；
- ・エンドユーザーがコンテンツ項目の一部を抽出し、その部分を他のエンドユーザーに再頒布することを許容し、該他のエンドユーザーがその部分にアクセスしうるようにする。これは、これらのエンドユーザーがコンテンツ項目全体に対するアクセス権を有するか否かによらない。
- ・エンドユーザーどうしが結託して、作品の一組の抜粋を連結することによって作品全体を自由に頒布することを困難にする。

【0005】

これはコンテンツを複数のブロックに分割し、各ブロックをそのコンテンツについてのマスター制御語から生成される制御語を使ってスクランブルすることによって有利に達成されうる。次いで、一つまたは複数のブロックが第一のエンドユーザーによって第二のエンドユーザーに送られることができ、それらのブロックには、マスター制御語ではなく、生成された制御語を含むライセンスが伴う。制御語生成のための好適なアルゴリズムを使えば、第二のエンドユーザーが当該コンテンツの他のブロックにアクセスできないことを確実にできる。

【0006】

従来技術は、制御語（暗号化鍵）生成のためのいくつかの解決策を提供している。

【0007】

たとえば特許文献1は、ブロックがハッシュ値を使って暗号化され、その後、暗号化されたブロックとハッシュ値がハッシュされて、後続ブロックを暗号化するために使われるハッシュ値を生成するシステムを記載している。さらに、特許文献2は、ブロックを、直前ブロックについて使われた鍵と組み合わせることによって鍵が得られる鍵生成システムを記載している。これらのシステムの問題は、復号を一つの「方向」に限定することが可能でないということである。

【先行技術文献】

【特許文献】

【0008】

【特許文献1】US2006/0034453

【特許文献2】EP2197145

【非特許文献】

【0009】

【非特許文献1】<http://www.copyright.gov/legislation/dmca.pdf> 40

【非特許文献2】Marc Joye and Sung-Ming Yen, One-Way Cross-Trees and Their Applications, D. Naccache and P. Pallier, Eds. Public Key Cryptography, vol.2274, Lecture Notes in Computer Science, pp.346-356, Springer Verlag, 2002

【非特許文献3】ISO/IEC13818-1, Information technology - Generic coding of moving pictures and associated audio information -- Part1: Systems, 2007

【非特許文献4】NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)," November 2001 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

【非特許文献5】S. Frankel, R. Glenn and S. Kelly, "The AES-CBC Cipher 50

Algorithm and Its Use with IPsec," RFC 3602, Internet Soc., Sept. 2003; <http://rfc.sunsite.dk/rfc/rfc3602.html>

【非特許文献6】R. Houseley, Use of the RSAES-OAEP Key Transport Algorithm in the Cryptographic Message Syntax (CMS), RFC 3560, July 2003

【非特許文献7】M. Bellare and P. Rogaway: Optimal Asymmetric Encryption - How to Encrypt with RSA. In: A. De Santis (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp.92-111. Springer, Heidelberg (1995)

【非特許文献8】RSA Laboratories, PKCS #1 v.2.1: RSA Cryptography Standard, June 2002

【発明の概要】

10

【発明が解決しようとする課題】

【0010】

上記の問題は、非特許文献2によってある程度は克服される。そのソリューションは、ある秘密から出発して、その左半分または右半分のいずれかがハッシュされて新しい秘密を生成し、それにより秘密の二分木を生成する。次いで各秘密は、たとえば、ハッシュされた鍵を生成してもよい。このソリューションは、いくつかの受け取った鍵からさらなる鍵を生成することを不可能にできる。木は鍵導出のための異なる経路を提供するが、プロセスは常に、木のあるノードから出発して低レベル・ノードへ降りていくというように、上から下の方向をたどる。

【課題を解決するための手段】

20

【0011】

本発明は、二つ以上の秘密を使い、それらについて導出プロセスが反対の方向になされる代替的なソリューションを提供する。これは、復号鍵の導出をいくつかの反対の「方向(direction)」に限定することを可能にする。

【0012】

第一の側面では、本発明は、コンテンツ項目の n 個の連続するユニットの暗号化または復号のための n 個の制御語を生成する装置に向けられる。ここで、 n は整数である。本装置は：第一の鍵 K_{start} および第二の鍵 K_{end} を取得し；前記第一の鍵 K_{start} に第一の一方方向性関数を逐次反復的に適用することによって n 個のサブ鍵の第一の順序付き集合を生成するとともに、前記第二の鍵 K_{end} に第二の一方方向性関数を逐次反復的に適用することによって n 個のサブ鍵の第二の順序付き集合を生成し； n 個のサブ鍵の前記第一の順序付き集合からのサブ鍵 i および n 個のサブ鍵の前記第二の順序付き集合からのサブ鍵 $n-i-1$ から制御語 i を生成する組み合わせ演算を逐次反復的に使うことにより n 個の制御語を生成し（ i は両端を含めて0から $n-1$ までの間）； n 個の生成された制御語を出力するよう適応されたプロセッサを有する。

30

【0013】

第一の好ましい実施形態では、前記第一の一方方向性関数および前記第二の一方方向性関数の少なくとも一方はハッシュ関数である。

【0014】

第二の好ましい実施形態では、前記第一の一方方向性関数および前記第二の一方方向性関数の少なくとも一方は公開鍵暗号化である。

40

【0015】

第三の好ましい実施形態では、前記組み合わせ演算はXORである。

【0016】

第四の好ましい実施形態では、前記組み合わせ演算は連結または公開鍵暗号化または対称鍵暗号化である。

【0017】

第五の好ましい実施形態では、前記プロセッサはさらに、コンテンツ項目をそれぞれ複数のユニットを含む複数の部分に分離し、各部分について独立に制御語を生成するよう適応される。

50

【0018】

第六の好ましい実施形態では、前記プロセッサはさらに、生成された制御語 i を使ってユニット i が暗号化されているコンテンツ項目についてのライセンスを生成し、前記ライセンスは前記第一の鍵 K_{start} 、前記第二の鍵 K_{end} および前記整数 n を含み；前記ライセンスを受信機に送信するよう適応されている。前記コンテンツ項目がより長いコンテンツ項目の抜粋であり、前記より長いコンテンツ項目が第三の鍵および第四の鍵から生成された制御語を使って暗号化され、前記プロセッサがさらに、前記第一の鍵 K_{start} を前記第一の一方方向性関数の前記第三の鍵への逐次反復的適用によって生成し、前記第二の鍵 K_{end} を前記第二の一方方向性関数の前記第四の鍵への逐次反復的適用によって生成するようさらに適応されていることが有利である。

10

【0019】

第七の好ましい実施形態では、前記コンテンツ項目は暗号化され、前記プロセッサはさらに、生成された制御語を使って暗号化されたコンテンツ項目を復号するよう適応されている。

【0020】

第二の側面では、本発明は、コンテンツ項目の n 個の連続するユニットの暗号化または復号のための n 個の制御語を生成する方法に向けられる。ここで、 n は整数である。ある装置が第一の鍵 K_{start} および第二の鍵 K_{end} を取得し；前記第一の鍵 K_{start} に第一の一方方向性関数を逐次反復的に適用することによって n 個のサブ鍵の第一の順序付き集合を生成するとともに、前記第二の鍵 K_{end} に第二の一方方向性関数を逐次反復的に適用することによって n 個のサブ鍵の第二の順序付き集合を生成し； n 個のサブ鍵の前記第一の順序付き集合からのサブ鍵 i および n 個のサブ鍵の前記第二の順序付き集合からのサブ鍵 $n-i-1$ から制御語 i を生成する組み合わせ演算を逐次反復的に使うことにより n 個の制御語を生成し（ i は0から $n-1$ までの間）； n 個の生成された制御語を出力する。

20

【0021】

第一の好ましい実施形態では、前記第一の一方方向性関数および前記第二の一方方向性関数の少なくとも一方はハッシュ関数である。

【0022】

第二の好ましい実施形態では、前記組み合わせ演算はXORである。

【0023】

第三の好ましい実施形態では、本方法はさらに、コンテンツ項目をそれぞれ複数のユニットを含む複数の部分に分離する段階を含み、本第二の側面の方法の各段階は、各部分について独立に実行される。

30

【0024】

第三の側面では、本方法は、前記第二の側面の方法によって生成された制御語を使って暗号化されているコンテンツ項目についてのコンテンツ・ライセンスを生成する方法に向けられる。ある装置が、生成された制御語 i を使ってユニット i が暗号化されているコンテンツ項目についてのライセンスを生成し、前記ライセンスは前記第一の鍵 K_{start} 、前記第二の鍵 K_{end} および前記整数 n を含み；前記ライセンスを受信機に送信する。

【0025】

第一の好ましい実施形態では、前記コンテンツ項目はより長いコンテンツ項目の抜粋であり、前記より長いコンテンツ項目は第三の鍵および第四の鍵から生成された制御語を使って暗号化され、本方法がさらに、前記第一の鍵 K_{start} を前記第一の一方方向性関数の前記第三の鍵への逐次反復的適用によって生成し、前記第二の鍵 K_{end} を前記第二の一方方向性関数の前記第四の鍵への逐次反復的適用によって生成する段階をさらに含む。

40

【図面の簡単な説明】

【0026】

本発明の好ましい特徴について、これから限定しない例として付属の図面を参照しつつ述べる。

【図1】本発明のある好ましい実施形態の例示的な使用分野を示す図である。

50

【図 2】本発明のある好ましい実施形態に基づくスクランブル装置を示す図である。

【図 3】本発明の第一の好ましい実施形態に基づくスクランブル鍵生成を示す図である。

【図 4】本発明の前記第一の好ましい実施形態に基づく抜粋生成、送信および受信を示す図である。

【発明を実施するための形態】

【0027】

本発明の主要な発想は、受信者に送達されることのできる少なくとも一つのスクランブル鍵（すなわち、暗号化および復号鍵）を生成しつつ、受信者が前記少なくとも一つのスクランブル鍵をさらなるスクランブル鍵を生成するために使用できないことを確実にすることである。

【0028】

例示的な使用分野が図 1 に示されている。コンテンツ項目 100 が複数のブロック 110 に分割されている。各ブロック (U_j) 110 はブロック指数 (j) によって同定される。ブロック指数は必須ではないが、有利には逐次的である。よってコンテンツ 100 はブロックの集合 $\{U_0, U_1, U_2, \dots, U_n\}$ を含む。

【0029】

コンテンツ 100 のスクランブル（暗号化とも呼ばれる）は図 2 を参照してさらに記述される。図 2 は、鍵生成器 210 およびスクランブラー 220 を含むスクランブル装置 200 を示している。スクランブル装置 200 は、一つまたは複数のプロセッサとして実装されてもよい。当業者は、対称暗号アルゴリズムについては暗号化および復号が本質的には同じであることを理解するであろう。同じ鍵および同じアルゴリズムを使って入力データを処理して出力データを生成するのである。

【0030】

コンテンツ 100 をスクランブルするために、そのブロック 110 は別個にスクランブルされる。鍵生成器 210 はスクランブルすべき各ブロック 110 についてブロック CW を生成する。鍵生成器 210 がそこから機能するブロック指数は、たとえばコンテンツ 110 から得られる最終ブロック指数まで、（指数が逐次的であれば）内部的に生成されてもよい。ブロック指数は、制御回路（図示せず）によってまたはスクランブラーによって、スクランブルすべきブロックの検査後に与えられてもよい。生成されたブロック制御語（control word） CW_j はスクランブラー 220 に届けられる。これは可能性としては対応するブロック指数と一緒にであってもよいが、スクランブラー 220 はブロック指数を制御回路から受け取ってもよい。さらなる可能性は、鍵生成器およびスクランブラーが同期されるということである。その場合、ブロック CW は、スクランブラーによって必要とされるときに届けられることができる。スクランブラー 220 はブロック U_j を受け取り、ブロック CW を使ってブロック U_j をスクランブルし、保護されたブロック（protected block） PU_j を出力する。

【0031】

このことは図 1 にも示されている。図 1 では、上の段のコンテンツ 110 のブロック U_j は、下の段の保護されたコンテンツ 120 の保護されたブロック PU_j 130 としてスクランブルされる。

【0032】

当業者は、スクランブル・アルゴリズムが対称的な場合にはスクランブラーとデスクランブラーの間には構造的な違いがないことを理解するであろう。実際、スクランブラーおよびデスクランブラーの両方は入力データを取り、本質的には同じアルゴリズムを同じ鍵とともに使って出力データを生成する。唯一の違いは、一方は平文を受けて暗号文を生成し、他方はその逆を行うということである。よって、図 2 は、適宜変更を施してスクランブル解除装置 200 をも示すことができる。

【実施例 1】

【0033】

〈第一の好ましい実施形態〉

10

20

30

40

50

本発明の第一の好ましい実施形態に基づき、図3はスクランブル鍵生成を示し、図4は抜粋生成、送信および受信を示す。二つの、好ましくはランダムなマスター鍵 K_{start} および K_{end} がコンテンツについて生成される。スクランブルすべきブロックの数が n であれば、各マスター鍵は一方方向性関数 h （有利にはハッシュ関数だが、可能性としては公開鍵暗号法の公開鍵を使う暗号化など他の関数であってもよい）によって少なくとも $n-1$ 回処理され、結果として各マスター鍵から生成される n 個のサブ鍵： $K_{s1}-K_{sn}$ および $K_{e1}-K_{en}$ を与える。例解のため、終端鍵（end key）はひっくり返されて、 K_{e1} が自らを終端に見出し、 K_{en} が自らを先頭に見出すと言ってもよい。

【0034】

次いで、各ブロックについて、鍵 K_{si} が鍵 $K_{e(n-i)}$ と組み合わせられてブロックCWを生成する。サブ鍵の長さがスクランブル・アルゴリズムによって必要とされる鍵長に対応する限り、組み合わせ演算は、實際上、公開鍵または対称鍵暗号化のような任意の算術演算、任意の二値演算、連結演算であることができる。好ましい組み合わせは排他的OR（XOR）である。

【0035】

数学的記法では、最初のブロックは指数〔インデックス〕0をもち、最後のブロックは指数 $n-1$ をもつ。各サブ鍵CWは次の公式によって二つのマスター鍵から生成される。

【0036】

【数1】

$$CW_i = h^i(K_{start}) \oplus h^{n-i}(K_{end}), i = 0 \dots n-1, \quad (式1)$$

ここで、 h は一方方向性関数、 h^m は該一方方向性関数の m 回の反復を表す。

【0037】

スクランブルされたコンテンツは次いでエンドユーザーに送信されてもよい。該エンドユーザーは、マスター鍵 K_{start} および K_{end} を含み、好ましくはユーザーに固有なユーザー鍵 K_u で暗号化された一般コンテンツ・ライセンスをも受け取ってもよい（必ずしもコンテンツと一緒にではなく）。非対称暗号システムでは、ユーザー鍵がユーザーの公開鍵であることが有利である。

【0038】

コンテンツをスクランブル解除するためには、ユーザーはまず、そのユーザー鍵 K_u （またはその対応する秘密鍵）を使ってライセンスを復号し、次いでマスター鍵 K_{start} および K_{end} を使ってコンテンツをスクランブル解除するために使われるサブ鍵を生成する。サブ鍵は式1の公式を使って生成される。

【0039】

第一のユーザーがコンテンツの抜粋、ブロック x からブロック $x+m$ までの $m+1$ 個の連続するブロック、を第二のユーザーと共有したいとき、第一のユーザーはこれらの連続するブロックを選択する（ステップS41）。第一のユーザー装置は次いで二つの派生鍵 K'_{start} および K'_{end} を生成する（ステップS42）：

$$K'_{start} = h^x(K_{start})$$

$$K'_{end} = h^{n-x-m}(K_{end})。$$

【0040】

K'_{start} は抜粋の最初のブロックについてのスクランブル鍵であり、 K'_{end} は抜粋の最後のブロックについてのスクランブル鍵であることが理解されるであろう。二つの派生鍵は次いで抜粋ライセンス中に埋め込まれる。抜粋ライセンスは第二のユーザーについての（対称または好ましくは非対称）暗号化鍵を使って暗号化される（ステップS43）。第一のユーザー装置は次いで抜粋および抜粋ライセンスを第二のユーザーに送る（ステップS44）。

【0041】

10

20

30

40

50

抜粋および抜粋ライセンスの受信に際して（ステップS45）、第二のユーザー装置は（対応する鍵を使って）抜粋ライセンスを復号する（ステップS46）。これらの派生鍵は次いで、式1と同様の公式（ K_{Start} の代わりに K'_{Start} 、 K_{End} の代わりに K'_{End} 、 i の代わりに x 、 $n-i$ の代わりに $n-x-m$ とする）を使って、 m 回ハッシュされ、組み合わせられて、抜粋の諸ブロックについてのサブ鍵を生成する（ステップ47）。

【0042】

別の言い方をすると、各サブ鍵は次のように計算される。

【0043】

【数2】

$$Kb_j = h^{i-x}(K'_{Start}) \oplus h^{x+m-j}(K'_{End}), j = x \dots x+m$$

抜粋は次いで、サブ鍵を使ってスクランブル解除され（ステップS48）、レンダリングされてもよい。

【0044】

本発明の鍵生成の利点は、抜粋の長さに関わりなく、抜粋ライセンスが二つの鍵のみを含むということである。これらの二つの（派生）鍵から、抜粋内のブロックについてのすべてのサブ鍵が簡単に計算できる。

【0045】

さらに、共有される部分内のサブ鍵を知っていても、抜粋外のサブ鍵の計算はできない。これらの「外部の」サブ鍵を計算するためには、 K'_{Start} の知識をもって指数 x に先行するブロックのサブ鍵を計算するとともに、 K'_{End} の知識をもって指数 $x+m$ より後のブロックのサブ鍵を計算することが必要である。だが、これは一方向性関数 h の逆を求めることを必要とし、計算量的に実現可能ではない。

【0046】

詳しくいうと、本第一の好ましい実施形態は、暗号化されていないコンテンツ・ストリームを入力として受け、該コンテンツ・ストリームは動画像専門家グループ2（MPEG2）コンテンツ・ストリームである。MPEG2はデジタル放送コンテンツ用のよく知られたエンコードおよび圧縮規格であり、非特許文献3に記載されている。

【0047】

MPEG2は、固定または可変サイズのフレームを含むパケット化されたエレメンタリー・ストリーム（PES: Packetized Elementary Streams）を含む。各PESパケットは、MPEG2トランスポート・ストリーム（TS: Transport Streams）として知られる、オーディオおよびビデオ・データの組み合わせを含む固定サイズの（188バイト）トランスポート・パケットに分解される。MPEG2コンテンツ・ストリームを保護するとき、各TSパケットは制御語（CW）で暗号化される。CWは10秒周期毎に変化する（つまり、暗号期間（crypto-period）が10s続く）。セットトップボックス・アーキテクチャでは、セットトップボックスのセキュリティ・モジュールが、暗号化されたCWを含む権限付与制御メッセージ（ECM: Entitlement Control Message）を受け取る。セキュリティ・モジュールは正しいCW（奇または偶）をデスクランブラー・モジュールに届け、該デスクランブラー・モジュールは次いで奇／偶CWを正しい時間にスクランブルされたTSに適用し、スクランブル解除されたTSパケットを出力する。

【0048】

各コンテンツ・プロバイダーは固有の秘密または公開情報 Ip を有しており、各ユーザーはセンターから証明された（certified）1024ビットのRSA鍵対（ K_{pub}, K_{priv} ）を受け取っている。コンテンツ・プロバイダー鍵 K_p はセンターによって知られており、ユーザー秘密鍵 K_{priv}_a および Ip はユーザーのセットトップボックス内に安全に格納されている。

【0049】

さらに、本第一の好ましい実施形態では：

10

20

30

40

50

- ・一方方向性関数 h はSHA1ハッシュ・アルゴリズムである。
- ・TSスクランブル・アルゴリズムはCBCモードのAES-128である。非特許文献4および5参照。
- ・ライセンス暗号化アルゴリズムは1024ビットの鍵長をもつRSA最適非対称暗号化パディング(OAEP: Optimal Asymmetric Encryption Padding)である。さらなる詳細については、非特許文献6、7、8を参照。

【0050】

例解用の例として、コンテンツは2時間の映画である。これは、コンテンツは $(2h) \times (60min/h) \times (60s/min) \times (1CW/10s) = 720$ 個のCW $CW_0 \sim CW_{719}$ を使ってスクランブルされることを意味する。

【0051】

さらに、 CW' および CW'' は、センターによってランダムに生成された二つの128ビットマスター鍵である。各 CW_i はこれら二つのマスター鍵から次の公式(式1を適応させたもの)を使って生成される。

【0052】

【数3】

$$CW_i = h^i(Ip || CW') \oplus h^{719-i}(Ip || CW''), i = 0 \dots 719$$

暗号期間 i 内のTSパケットが $TS_ENC = AES-128-ENC'(CW_i, TS)$ とスクランブルされる。SHA1の出力が160ビットであることを与えられると、 CW_i も160ビットである。AES鍵サイズ(128ビット)を適合させるためには、各 CW_i は、たとえば上位32ビットまたは下位32ビットを破棄することによって、128ビットに打ち切られる。

【0053】

マスター鍵 CW' および CW'' は一つの $ECM = \{CW', CW''\}$ 内に埋め込まれる。このECMは128ビットのプロバイダー識別子(provider identifier)情報(PID)をも含む。PIDは、どのプロバイダー情報 Ip をどのコンテンツと一緒に使うべきかを知る助けになる。ECMはまた、必要なCWの総数をも含む(この2バイト・フィールドはハッシュ指数[インデックス]を計算する助けになる)。コンテンツをユーザーに配送する前に、400ビットの $ECM = \{CW', CW'', CW_count=720, PID\}$ がユーザーの公開鍵 $Kpub_a$ を用いて暗号化される。すなわち、 $ECM_ENC = RSA-1024-ENC(Kpub_a, ECM)$ となる。

【0054】

コンテンツをスクランブル解除するためには、セキュリティ・モジュールは秘密ユーザー鍵 $Kpriv_a$ を使ってECMを解読する。次いで、PID情報を使って、セキュリティ・モジュールはどのプロバイダー情報 Ip を使うべきかを知る。セキュリティ・モジュールは次いで、センターと同じCW生成アルゴリズムを使って、マスター鍵 CW' および CW'' 、プロバイダー情報 Ip および CW_count から、保護されるマルチメディア・コンテンツを構成するスクランブルされたTSパケットのための制御語 CW_i を生成する。

【0055】

CW計算を少なく保つために、すなわち同じ値を数回生成するのを避けるために、CWを次のようにして生成するのが有利である：

1. マスター制御語 CW' および CW'' を受信すると、 CW'' からすべての制御語の「第二の部分」を生成する

$$CW''_i = h^{619-i}(Ip || CW'')$$

ここで、 i は $CW_count - 1 = 619$ で始まり、0に達するまでデクリメントされる。

2. これら第二の部分をメモリ中のリスト L 内に、第一のCW、 $CW' = CW'_0$ の「第一の部分」と一緒に保存する。

【0056】

$$L = \{CW', CW''_0, CW''_1, \dots, CW''_{619} = CW''\}$$

10

20

30

40

50

(これは2時間の映画については約12kb ($721 \times 16 = 11586$ バイト)のメモリを必要とする。)

3. 第一のCWを計算するために、
【数4】

$$CW_0 = CW'_0 \oplus CW''_0$$

を計算する。ここで、 CW'_0 および CW''_0 はLから取り出された。

4. 次の制御語の第一の部分によってリストL中の CW'_0 を更新する。すなわち、 $CW'_0 \leftarrow h(Ip \parallel CW') = CW_1$ となる。

5. スランブルされた各TSパケットについて、ステップ3～4を、最終的なCWが生成されるまで繰り返す。

【0057】

【数5】

$$CW_{619} = CW'_{619} \oplus CW''_{619}$$

当業者は、この方法が若干のメモリ・スペースを必要とするが、多くの計算ステップを節約することを理解するであろう。

【0058】

第一のユーザーが、コンテンツの、映画の開始から60分のところに位置する10分の抜粋を第二のユーザーと共有したいとする。10分の抜粋は $6 \times 10 = 60$ 個のCWを使ってスランブルされている。抜粋の始まりおよび終わりのCWはそれぞれ CW_{360} および CW_{419} である。

【0059】

この抜粋について、第一のユーザーのセキュリティ・モジュールはマスター鍵 CW' および CW'' から二つの抜粋鍵 CW_e' および CW_e'' を次のように生成する。

【0060】

$$CW_e' = h^{360}(Ip \parallel CW')$$

$$CW_e'' = h^{619-419}(Ip \parallel CW'') = h^{200}(Ip \parallel CW'')$$

【0061】

鍵 CW_e' および CW_e'' は抜粋ECM(excerpt ECM)に埋め込まれる。 $EECM = \{CW_e', CW_e'', CW_count = 60, PID\}$ 。スランブルされた抜粋を第二のユーザーに頒布する前に、セキュリティ・モジュールはEECMを第二のユーザーの公開鍵 K_{pub_b} を用いて暗号化する。すなわち、 $EECM_ENC = RSA-1024-ENC(K_{pub_b}, EECM)$ となる。

【0062】

スランブルされた抜粋を受領すると、第二のユーザーのセキュリティ・モジュールは第二のユーザーの秘密鍵 K_{priv_b} を使って1024ビットのEECM_ENCを解読する。次いで、当該部分内の暗号期間j内のTSパケットについての各制御語 CW_j が次のように計算される。

【0063】

【数6】

$$CW_j = h^j(Ip \parallel CW_e') \oplus h^{59-j}(Ip \parallel CW_e''), j = 0 \dots 59$$

これらの制御語を使って、スランブルされた抜粋がスランブル解除され、ユーザーに対してレンダリングされる。

【0064】

当業者は、従来技術のシステムでは、スランブル／デスランブルのために使われるCWはランダムに生成されたものであり、互いに独立であったことを認識するであろう。セキュリティ・モジュールは各TSパケットについてECMを受け取り、解読しなければならなかった。これは、保護されたコンテンツについて処理すべき数百のECMとなる(2時間の

10

20

30

40

50

映画については少なくとも720個のECM)。しかしながら、本発明の第一の実施形態によれば、セキュリティ・モジュールはコンテンツ当たり単一のECMまたはEECMを必要とするだけである。そのECM/EECMを使ってコンテンツのスクランブル解除に必要なCWを生成することが可能だからである。よって、本発明の第一の実施形態が伝送帯域幅を節約できることが理解されるであろう。・

【実施例 2】

【0065】

〈第二の好ましい実施形態〉

前記第一の好ましい実施形態によって提供されるソリューションはコンパクトだが、結託攻撃に対する耐性はない。コンテンツの二つの連続しない抜粋へのアクセスをもつ攻撃者は、二つの抜粋の間にあるすべてのパケットについての制御語を生成できる。それらの抜粋がコンテンツの始まりと終わりに対応する場合には、そのコンテンツについてのすべての制御語が生成されうる。

【0066】

第二の好ましい実施形態は、コンテンツを複数の論理的な部分に分離することによって、結託攻撃に対する耐性を提供する。各部分は、コンテンツ全体より少なく、単一のブロックよりは多いものを含む。例解用の例として、各部分は10分（すなわち60ブロック）の長さであるが、これより短いまたは長いのもよい。

【0067】

各部分についての制御語は、あたかも各部分がコンテンツ項目全体であるかのように、他の部分についての制御語とは独立に生成される。

【0068】

換言すれば（映画の例を続けると）、映画コンテンツの10分毎に、センターは二つの128ビットのマスター鍵 $CW'[k]$ および $CW''[k]$ を生成する、 $k=0\cdots 11$ （これは2時間の映画について24個のマスター鍵を表す）。各 $CW_i[k]$ はこれらのマスター鍵から次の公式を使って生成される。

【0069】

【数 7】

$$CW_i[k] = h^i(lp||CW[k]) \oplus h^{59-i}(lp||CW''[k]), i=0\cdots 59, k=0\cdots 11$$

これは二つの型の周期を生じさせることが見て取れる：CWが変化する（kが固定されたままの間、公式中の指数iが変化する）10秒の下位暗号期間と、マスター鍵 CW' および CW'' が変化する（公式中の指数kが変化する；この期間の先頭でiは0にリセットされる）10分の上位暗号期間である。

【0070】

暗号期間 $\{i, k\}$ 内のTSパケットは $TS_ENC = AES-128-ENC(CW_i[k], TS)$ としてスクランブルされる。

【0071】

この場合、コンテンツ全体について一つの一意的なECMを有する代わりに、それぞれ異なるマスター鍵の対を含む12個のECMがある： $ECM_k = \{CW'[k], CW''[k], CW_count=60, PID\}$ 。 CW_count がしかるべく調整される限り、これらの部分が異なる長さであることも可能であることを注意しておくべきである。

【0072】

ユーザーが10分より短い抜粋のみ共有できる場合、一つのEECMを送信することが必要なだけである。第一のユーザーがコンテンツの5分の部分を第二のユーザーと共有したいとする。その部分は、映画の始まりから60分のところに位置されている。5分の抜粋はマスター鍵 $\{CW'[6], CW''[6]\}$ （抜粋は「上位」暗号期間7に位置しているので）から導出される $6 \times 5 = 30$ 個のCWによって保護される。この抜粋の始まりおよび終わりのCWはそれぞれCW

10

20

30

40

50

$o[6]$ および $CW_{29}[6]$ である。

【0073】

セキュリティ・モジュールは、マスター鍵 $CW'[6]$ および $CW''[6]$ から二つの鍵 CW_p' および CW_p'' を次のように生成する。

【0074】

$$CW_p' = h^0(Ip \parallel CW'[6]) = CW_0[6] = CW'[6]$$

$$CW_p'' = h^{5^9 \cdot 2^9}(Ip \parallel CW''[6]) = h^{3^0}(Ip \parallel CW''[6])。$$

【0075】

鍵 CW_p' および CW_p'' は次いで $EECM = \{CW_p', CW_p'', CW_count = 30, PID\}$ に埋め込まれる。保護された抜粋を第二のユーザーに頒布する前に、EECMは第二のユーザーの公開鍵 $Kpub_b$ を使って暗号化される。すなわち、 $EECM_ENC = RSA-204-ENC(Kpub_b, EECM)$ となる。

10

【0076】

保護された抜粋を受領すると、第二のユーザーのセキュリティ・モジュールは第二のユーザーの秘密鍵 $Kpriv_b$ を使って1024ビットの $EECM_ENC$ を解読し、次いで、諸暗号期間 $\{j, 6\}$ 内のTSパケットについての制御語 $CW_j[6]$ を次のように生成する。

【0077】

【数8】

$$CW_j[6] = h^j(Ip \parallel CW_p') \oplus h^{29^j}(Ip \parallel CW_p''), j = 0 \dots 29$$

20

抜粋を本発明の第二の好ましい実施形態を使って保護すると、コンテンツの二つの連続しない抜粋へのアクセスをもつ攻撃者は、それらの抜粋が同じマスター鍵の暗号期間に属するのでない限り、それら二つの抜粋の間に位置されるTSパケットについての制御語を再構築することができない。

【0078】

本発明は、プロセッサによって実行されたときに該プロセッサに本発明の方法を実行させる命令を記憶するDVDまたはCD-ROMのようなコンピュータ・プログラム・プロダクトにも関係する。

【0079】

本発明が、受領者に対してコンテンツ全体を利用可能にすることなく、ユーザーが保護されたコンテンツの一部を共有することを可能にできることは理解されるであろう。本発明のソリューションは、計算コストの点で効率的であり、帯域幅効率がよく（より少ないデータが転送される）、第二の実施形態では結託攻撃に耐性があることができる。それによって同時に、実際上任意の既存のコピー保護システムとともに実装できる。

30

【0080】

本稿および（該当する場合には）請求項および図面で開示される各特徴は、独立して、あるいは任意の適切な組み合わせにおいて提供されてもよい。請求項に現れる参照符号は単に例解のためであって、特許請求の範囲に対する限定する効果はもたない。

【符号の説明】

40

【0081】

100 コンテンツ

110 ブロック

120 保護されたコンテンツ

130 保護されたブロック

200 スクランブル装置

210 鍵発生器

220 スクランプラー

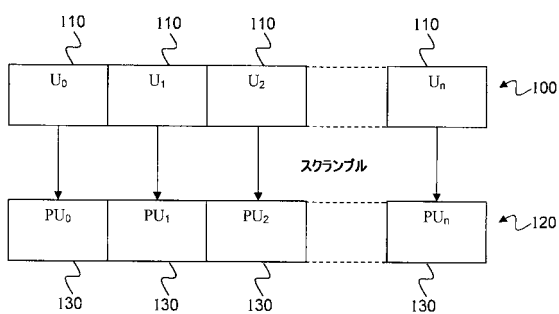
S41 送信すべき抜粋を選択

S42 抜粋鍵を生成

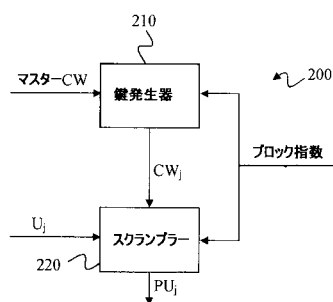
50

- S43 抜粋ライセンスを生成
 S44 抜粋および抜粋ライセンスを送信
 S45 抜粋および抜粋ライセンスを受信
 S46 抜粋ライセンスを解読
 S47 制御語を生成
 S48 抜粋をスクランブル解除

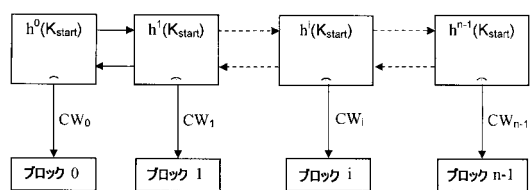
【図 1】



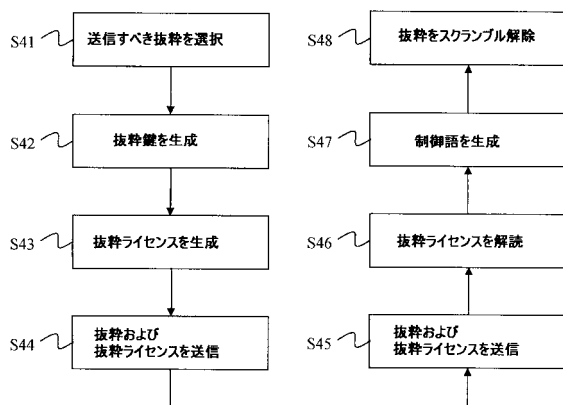
【図 2】



【図 3】



【図 4】



フロントページの続き

(72)発明者 モハメド カロウミ

フランス国 3 5 5 1 0 セゾン・セヴィニエ アヴェニュー・ド・ベル・フォンテーヌ 1 テク
ニカラー・アールアンドディー・フランス

Fターム(参考) 5J104 AA16 AA32 EA04 EA18 JA03 NA02 NA37 PA14

【外国語明細書】
2012170066000001.pdf