SCIS 2012 The 29th Symposium on
Cryptography and Information Security
Kanazawa, Japan, Jan. 30 - Feb. 2, 2012
The Institute of Electronics,
Information and Communication Engineers

# メディアアクセス制御のための再帰ハッシュ連鎖型多次元鍵派生方式
# A Multidimensional Key Derivation Scheme for Media Access Control Using Recursive Hash Functions

今泉 祥子 * 青木 直和 * 小林 裕幸 * 貴家 仁志 †
Shoko IMAIZUMI Naokazu AOKI Hiroyuki KOBAYASHI Hitoshi KIYA

**あらまし** 本稿では，再帰ハッシュ連鎖を用いた多次元暗号鍵派生方式とメディアコンテンツに対する階層的アクセス制御への適用を提案する．提案法は，あるハッシュ連鎖による出力値を別のハッシュ連鎖の構築に利用する，再帰ハッシュ連鎖を用いることによって，制御対象となるメディアの個数，各メディアの品質尺度の種類（次元），および，品質尺度の階層数に関わらず，管理鍵を常に一つとする．また，提案法は，暗号鍵派生順序を改善し，各暗号鍵の独立性を向上させることより，複数の不正ユーザが互いの鍵を共有し，許諾されていない高品質でのコンテンツ再生を企てる結託攻撃に対して耐性を考慮している．

**キーワード** 鍵派生　ハッシュ連鎖　アクセス制御　メディアコンテンツ　排他的論理和

## 1 まえがき

近年，通信路や通信端末の多様化に伴い，コンテンツ配信サービスでは，ユーザごとの個々の要求に応じて，異なった品質でのコンテンツ提供が求められている．例えば，テレビジョン放送において，ワンセグ放送では 15 fps，高精細度テレビジョン放送では 30 fps，60 fps などのように，再生環境に応じたフレームレートでコンテンツ再生が可能となっている．有料配信の場合，課金の額は再生されるコンテンツの品質ごとに異なるため，再生品質に基づくアクセス制御が要求される．この要求に対応するため，コンテンツの品質は階層化され，さらに，各階層ごとに暗号化される．本稿では，再生品質に多次元の階層構造を有するメディアコンテンツのアクセス制御のための暗号鍵派生方式を提案する．

暗号化に基づくアクセス制御では，再生品質に応じたアクセス制御を実現するため，階層を構成する単位データごとに異なる暗号鍵を割り当てる．単純な方式として，単位データごとに互いに独立な暗号鍵を割り当てる方式 [1] や，高品質再生用の暗号鍵が，より低品質用の暗号鍵の鍵情報をすべて包含する方式 [2] などがある．これらの方式では，サービス事業者が管理する鍵（以下，管理鍵と呼ぶ）の個数が膨大になると同時に，再生品質が高いほど，ユーザが受信する鍵（以下，配送鍵と呼ぶ）の個数が増加するという問題が生じる．

この問題に対応するため，鍵派生にハッシュ連鎖 [3] を用いることによって，管理鍵および配送鍵の個数を削減する方法が検討されている [4–7]．著者らは，一つのコンテンツに複数のメディアが存在するメディアコンテンツを対象に，メディアの品質尺度に階層構造を設定して，アクセス制御を施すための研究を行ってきた [9,10]．従来法 [9] は，暗号鍵の派生に再帰ハッシュ連鎖を用いることにより，メディアの個数に関わらず，管理鍵を 1 個とする暗号鍵派生方式である．しかし，この手法 [9] では，メディアコンテンツを構成する複数のメディアのうち，一つのメディアの品質尺度にしか階層構造を設定できない．そこで従来法 [10] は，従来法 [9] と同様に管理鍵を 1 個としたまま，各メディアにつき一つの品質尺度に階層構造を設定可能とした．しかしながら，この手法 [10] では，一つのメディアの複数の品質尺度に同時に階層構造を設定し，アクセス制御を施すことができない．ただし，これらの手法 [9,10] では，複数ユーザが互いの鍵を共有することで，許諾されていない高品質での不正再生を企てる，結託攻撃に対して耐性が考慮されている．

そこで本稿では，メディアコンテンツを構成する個々

* 千葉大学大学院融合科学研究科，〒 263–8522 千葉県千葉市稲毛区弥生町 1–33, Graduate School of Advanced Integration Science, 1–33 Yayoicho, Inage-ku, Chiba-shi, Chiba 263–8522 Japan, imaizumi@chiba-u.jp
† 首都大学東京システムデザイン学部，〒 191–0065 東京都日野市旭ヶ丘 6–6, Department of Information and Communication Systems, Tokyo Metropolitan University, 6–6 Asahigaoka, Hino-shi, Tokyo 191–0065 Japan

のメディアについて，複数の品質尺度に階層構造を設定可能な，メディアコンテンツのアクセス制御のための暗号鍵派生方式を提案する．提案法は，従来法と同様に，管理鍵を 1 個のみとし，結託攻撃に対して耐性を有している．また，従来法 [9] では，最高品質での再生を許諾されたユーザに管理鍵を配送していたのに対して，提案法では，管理鍵はいずれのユーザに対しても配送されることがない．

## 2 想定するメディアコンテンツの階層構造

本節では，提案法で扱うメディアコンテンツの制御対象の階層構造について，従来法 [10] における階層構造と比較しながら説明する．本稿で扱うアクセス制御の制御対象は，画像，音声，テキストなどのメディアから構成されるマルチメディアコンテンツであり，個々のメディアごとにアクセスの可否を制御する．さらに，本稿では，各メディアの複数の品質尺度（例えば，画像の場合，解像度，フレームレートなど）に階層構造を設定し，いずれの階層に対しても，同時にアクセス制御を施すことを想定する．

$M$ 個のメディア $S_i$ $(i = 1,2,\ldots,M)$ から構成されるメディアコンテンツ $C$ を仮定する．メディア $S_i$ の $Q_i$ 個の品質尺度 $G_i^{q_i}$ に対して $N_i^{q_i}$ 層 $(q_i = 1,2,\ldots,Q_i)$ の階層構造をそれぞれ設定する．ただし，品質尺度 $G_i^{q_i}$ の階層数の関係は，$N_i^1 > N_i^2 > \cdots > N_i^{Q_i}$ とする．このとき，メディアコンテンツ $C$，個々のメディア $S_i$，および，階層構造が設定された品質尺度 $G_i^{q_i}$ の階層 $G_i^{q_i,j}$ $(j = 1,2,\ldots,N_i^{q_i})$ の相互関係は，

$$C = \{S_1, S_2, \ldots, S_M\} \tag{1}$$

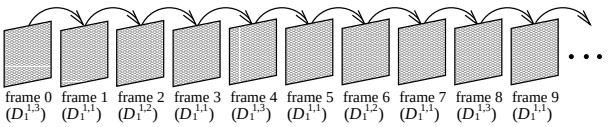
$$S_i = \{G_i^{1,1}, G_i^{2,1}, \ldots, G_i^{Q_i,1}\}, \qquad i = 1,2,\ldots,M \tag{2}$$

$$G_i^{q_i,1} \supset G_i^{q_i,2} \supset \cdots \supset G_i^{q_i,N_i^{q_i}}, \qquad q_i = 1,2,\ldots,Q_i \tag{3}$$

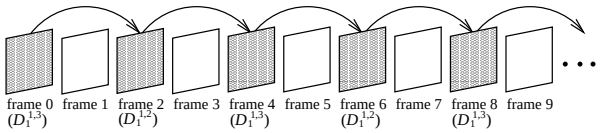
とそれぞれ表される．また，$E_i^{q_i}$ を $G_i^{q_i}$ の補集合とすると，その関係は次式で与えられる．

$$E_i^{q_i,j} = \begin{cases} G_i^{q_i,j} - G_i^{q_i,j+1}, & j = 1,2,\ldots,N_i^{q_i} - 1 \\ G_i^{q_i,j}, & j = N_i^{q_i} \end{cases}$$
$$i = 1,2,\ldots,M, \quad q_i == 1,2,\ldots,Q_i, \tag{4}$$

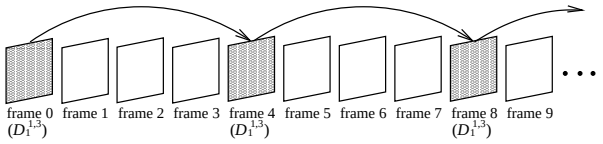
ここで，メディア $S_1$ を画像，制御対象の品質尺度 $G_1^1$ をフレームレートとし，図 1 に示す動画像を例にして，上述の階層条件について補足する．同図では，3 種類のフレームレート（$N_1^1 = 3$），15 fps（同図 (c)），30 fps（同図 (b)），および，60 fps （同図 (a)）を仮定する．まず，集合 $G_1^{1,1}$ は，フレームレートが最も高い 60 fps のフレーム集合である．続いて，30 fps のフレーム集合が $G_1^{1,2}$，15 fps のフレーム集合が $G_1^{1,3}$ となる．したがって，




(a) 60 fps（集合 $G_1^{1,1}$）




(b) 30 fps（集合 $G_1^{1,2}$）




(c) 15 fps（集合 $G_1^{1,3}$）

図 1: 各フレームレートにおける動画像再生（影部フレームを再生）

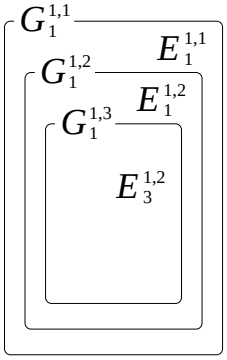



図 2: 図 1 における集合関係

これらの集合は，

$$G_1^{1,1} \supset G_1^{1,2} \supset G_1^{1,3} \tag{5}$$

の関係で示され，これは式 (3) の階層条件を満たしている．

また，集合 $G_1^{1,1}$ のうち，60 fps 時のみ再生されるフレームの集合が $E_1^{1,1}$，集合 $G_1^{1,2}$ のうち，15 fps では再生されないフレームの集合が $E_1^{1,2}$ となる．なお，集合 $G_1^{1,3}$ はフレーム集合 $E_1^{1,2}$ に等しい．これらの関係は式 (4) のとおりであり，図 2 のように表される．階層的アクセス制御において，暗号化処理は，階層を構成する $N_i^{q_i}$ 個の単位データごとに施される．この例では，図 1 に示すとおり，フレーム集合 $E_1^{1,1}$，$E_1^{1,2}$，$E_1^{1,3}$ が単位データ $D_1^{1,1}$，$D_1^{1,2}$，$D_1^{1,3}$ に相当する．各単位データは，$D_1^{1,1}$，$D_1^{1,2}$，$D_1^{1,3}$ の順で復号される．

従来法 [10] では，各メディア $S_i$ につき 1 個（$Q_i = 1$）の品質尺度 $G_i^1$ にのみ階層構造を設定可能である．したがって，従来法 [10] において，上式 (1)，(2)，(3) を満たすメディアコンテンツ $C$ の例は，図 3 のように表され

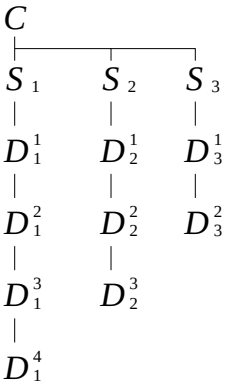



図 3: 従来法 [10] におけるメディアコンテンツの構成例

る．一方，次節で提案する方式で扱うメディアコンテンツ $C$ は，各メディア $S_i$ につき複数の品質尺度 $G_i^{q_i}$（$q_i$ は 2 以上の整数）に階層構造を設定可能である．このとき，式 (1)，(2)，(3) を満たすメディアコンテンツ $C$ の例を図 4 に示す．同図において，メディアコンテンツ $C$ は，3 個のメディア $S_1$，$S_2$，$S_3$ から構成され（$M=3$），各メディアはそれぞれ複数の品質尺度に基づき，式 (1)，(2)，(3) を満たすような階層構造が設定されている（$N_1^1=4$，$N_1^2=3$，$N_1^3=2$，$N_2^1=4$，$N_2^2=3$，$N_3^1=3$，$N_3^2=2$）．提案法は，従来法 [10] 同様，管理鍵をただ一つとし，かつ，結託攻撃耐性を有する．

## 3 提案法

メディアコンテンツを構成する個々のメディアに，複数の品質尺度に階層構造を設定可能とするアクセス制御方式において，管理鍵を 1 個のみとし，かつ，結託攻撃耐性を有する暗号鍵派生法について説明する．

図 4 のメディアコンテンツに対応した暗号鍵派生アルゴリズムを図 5 に示す．図 5 において，例えば，$K_{D_1^{4,1,1}}$ は図 4 に示すメディア $S_1$ の単位データ $D_1^{4,1,1}$ に，$K_{D_2^{1,3}}$ はメディア $S_2$ の単位データ $D_2^{1,3}$ に，それぞれ対応する暗号鍵である．ここで，$K_C$ が提案法における唯一の管理鍵であり，いずれの単位データの暗号鍵としても用いられない．

まず，次式に示すように，管理鍵 $K_C$ に対してハッシュ演算を施したものを，メディア $S_1$ に対する初期鍵 $K_{S_1}$ とする．

$$K_{S_1} = H(K_C) \tag{6}$$

ハッシュ演算およびハッシュ連鎖は，図 5 において黒矢印で示されている．次に，$K_C$ と式 (6) より $K_C$ のハッシュ値として算出された $K_{S_1}$ を用いて，

$$\begin{aligned} K_{S_2} &= H(F(K_C, K_{S_1})) \\ &= H(F(K_C, H(K_C))) \end{aligned} \tag{7}$$

より，メディア $S_2$ に対する初期鍵 $K_{S_2}$ を算出する．ここで，関数 $F()$ は結合関数を表しており，例として排他的論理和（XOR）が挙げられる．さらに，$K_{S_1}$ と $K_{S_2}$ を用いて，式 (7) と同様，

$$\begin{aligned} K_{S_3} &= H(F(K_{S_1}, K_{S_2})) \\ &= H(F(H(K_C), H^2(K_C))) \end{aligned} \tag{8}$$

により，メディア $S_3$ に対する初期鍵 $K_{S_3}$ を算出する．ここで，$H^b(a)$ は，$a$ に対してハッシュ演算を $b$ 回施す，ハッシュ連鎖 [3] を意味している．上式 (7)，(8) に示すように，提案法では，算出されたハッシュ値を再度用いることで，すなわち，再帰ハッシュ連鎖を用いることで，各メディアの初期鍵をそれぞれ派生している．図 5 において，再帰ハッシュ連鎖は白矢印で示されている．

これら三つのメディア $S_1$，$S_2$，$S_3$ の各単位データ $D_1^{n_1^1,n_1^2,n_1^3}$，$D_2^{n_2^1,n_2^2}$，$D_3^{n_3^1,n_3^2}$ に対する暗号鍵 $K_{D_1^{n_1^1,n_1^2,n_1^3}}$，$K_{D_2^{n_2^1,n_2^2}}$，$K_{D_3^{n_3^1,n_3^2}}$ $\left(n_i^{q_i}=1,2,\ldots,N_i^{q_i}\right)$ は，式 (6)，(7)，(8) で派生された $K_{S_1}$，$K_{S_2}$，$K_{S_3}$ から，ハッシュ連鎖と再帰ハッシュ連鎖を組合せて用いることで従属的に派生される．ここでは，メディア $S_1$ の単位データ $D_1^{n_1^1,n_1^2,n_1^3}$ に対する暗号鍵 $K_{D_1^{n_1^1,n_1^2,n_1^3}}$ を例に説明する．

まず，階層数が最も小さい，すなわち，$N_i^3$ の品質尺度 $G_i^3$ 方向の暗号鍵 $K_{D_1^{1,1,2}}$ は，

$$\begin{aligned} K_{D_1^{1,1,2}} &= H\left(F\left(K_{D_1^{1,1,1}}, K_{D_1^{1,2,1}}\right)\right) \\ &= H\left(F\left(K_{D_1^{1,1,1}}, H\left(F\left(K_{D_1^{1,1,1}}, K_{D_1^{2,1,1}}\right)\right)\right)\right) \\ &= H\left(F\left(K_{D_1^{1,1,1}}, H\left(F\left(K_{D_1^{1,1,1}}, H\left(K_{D_1^{1,1,1}}\right)\right)\right)\right)\right) \end{aligned} \tag{9}$$

のとおり，再帰ハッシュ連鎖の利用により，それぞれ派生される．次に，階層数が 2 番目に小さい，すなわち，$N_i^2$ の品質尺度 $G_i^2$ 方向の暗号鍵 $K_{D_1^{1,2,1}}$，$K_{D_1^{1,3,1}}$ は，

$$\begin{aligned} K_{D_1^{1,2,1}} &= H\left(F\left(K_{D_1^{1,1,1}}, K_{D_1^{2,1,1}}\right)\right) \\ &= H\left(F\left(K_{D_1^{1,1,1}}, H\left(K_{D_1^{1,1,1}}\right)\right)\right) \end{aligned} \tag{10}$$

$$\begin{aligned} K_{D_1^{1,3,1}} &= H\left(F\left(K_{D_1^{1,2,1}}, K_{D_1^{2,2,1}}\right)\right) \\ &= H\left(F\left(K_{D_1^{1,2,1}}, H\left(K_{D_1^{1,2,1}}\right)\right)\right) \end{aligned} \tag{11}$$

のとおり，式 (9) 同様，再帰ハッシュ連鎖を用いることによって派生される．なお，上式 (9) は，

$$\begin{aligned} K_{D_1^{1,1,n_1^3}} &= H\left(F\left(K_{D_1^{1,1,n_1^3-1}}, K_{D_1^{1,2,n_1^3-1}}\right)\right) \\ &= H\left(F\left(K_{D_1^{1,1,n_1^3-1}}, \right.\right. \\ &\qquad \left.\left. H\left(F\left(K_{D_1^{1,1,n_1^3-1}}, K_{D_1^{2,1,n_1^3-1}}\right)\right)\right)\right) \end{aligned}$$

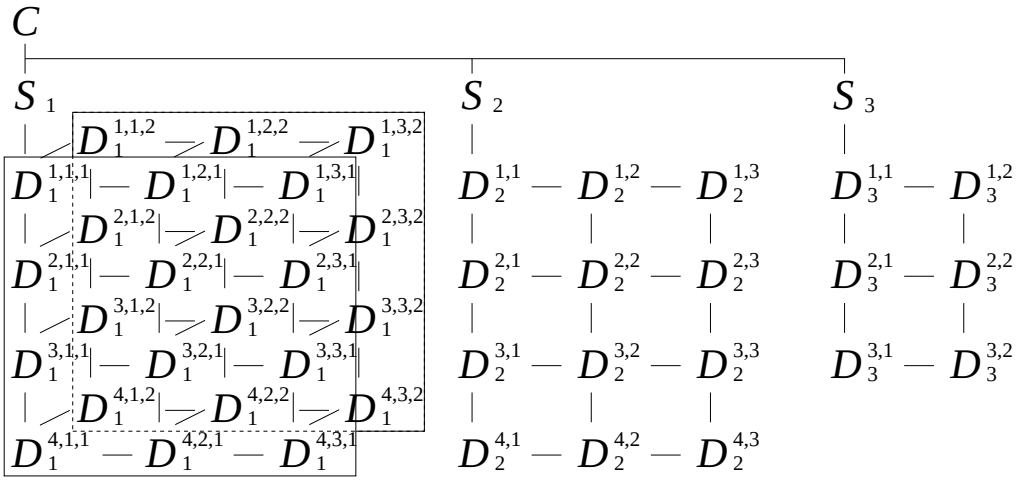


図 4: 想定するメディアコンテンツの構成例

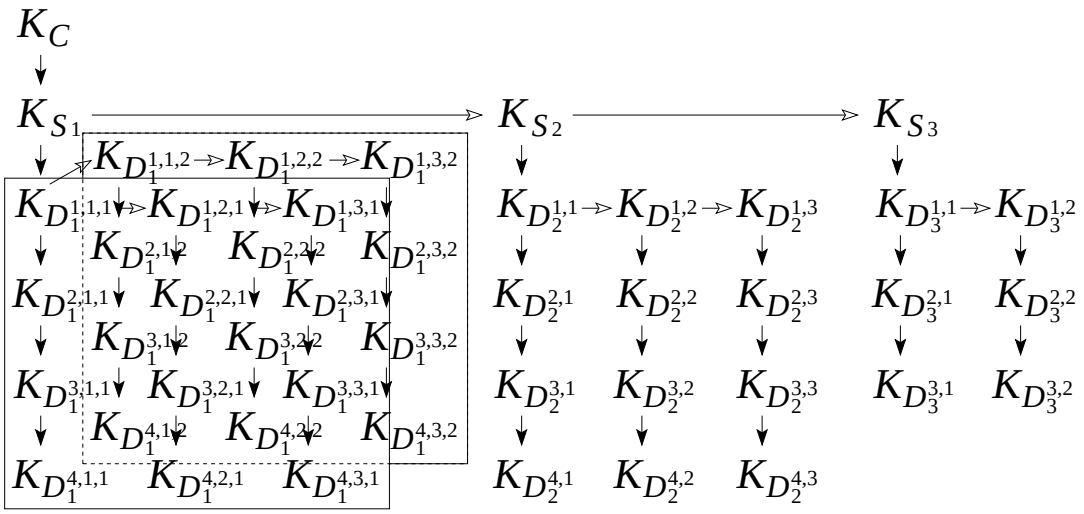


図 5: 暗号鍵派生アルゴリズム（黒矢印はハッシュ連鎖，白矢印は再帰ハッシュ連鎖）

$$= H\left(F\left(K_{D_1^{1,1,n_1^3-1}},\right.\right.$$
$$\left.\left.H\left(F\left(K_{D_1^{1,1,n_1^3-1}}, H\left(K_{D_1^{1,1,n_1^3-1}}\right)\right)\right)\right)\right)$$
$$n_1^3 = 2,3,\ldots,N_1^3 \tag{12}$$

のとおり，一方，式 (10)，(11) は，各 $n_1^3$ について，

$$K_{D_1^{1,n_1^2,n_1^3}} = H\left(F\left(K_{D_1^{1,n_1^2-1,n_1^3}}, K_{D_1^{2,n_1^2-1,n_1^3}}\right)\right)$$
$$= H\left(F\left(K_{D_1^{1,n_1^2-1,n_1^3}}, H\left(K_{D_1^{1,n_1^2-1,n_1^3}}\right)\right)\right),$$
$$n_1^2 = 2,3,\ldots,N_1^2 \tag{13}$$

のとおり一般化される．

また，階層数が最も大きい，すなわち，$N_i^1$ の品質尺度 $G_i^1$ 方向の暗号鍵 $K_{D_1^{n_1^1,n_1^2,n_1^3}}$ は，式 (13) で派生された暗号鍵 $K_{D_1^{1,n_1^2,n_1^3}}$ を初期値として，各 $n_1^2$，$n_1^3$ について，

$$K_{D_1^{n_1^1,n_1^2,n_1^3}} = H\left(K_{D_1^{n_1^1-1,n_1^2,n_1^3}}\right)$$
$$= H^{n_1^1-1}\left(K_{D_1^{1,n_1^2,n_1^3}}\right)$$
$$n_1^1 = 2,3,\ldots,N_1^1 \tag{14}$$

のとおり，ハッシュ連鎖を用いて，それぞれ従属的に派生される．

このように，提案法は，ハッシュ連鎖と再帰ハッシュ連鎖を組合せて用いることで，各メディアの複数の品質尺度に階層構造を設定しても，一つの管理鍵から各単位データに対する暗号鍵を派生可能である．また，提案法は，あらゆる結託攻撃に対して耐性を考慮している．図 5 に示すとおり，各メディアを関連付ける暗号鍵は，いずれの単位データにも割り当てられず，各メディアは，見かけ上，それぞれ独立な暗号鍵で暗号化される．また，

表 1: 提案法と従来法 [9, 10] との比較

| | 提案法 | 従来法 [9] | 従来法 [10] |
|---|---|---|---|
| 管理鍵の個数 | 1 | 1 | 1 |
| 結託攻撃耐性 | 有 | 有 | 有 |
| 階層構造の設定 | 複数メディアの複数品質 | 単一メディアの単一品質 | 複数メディアの単一品質 |
| 管理鍵の配送 | 無 | 有 | 無 |

いずれの品質尺度の階層についても，下位の階層から上位の階層に対する暗号鍵は派生できない．これにより，複数ユーザが互いの暗号鍵を共有し，組合せて用いても，許諾されていない単位データに対する暗号鍵は派生することはできない．このように，提案法は，許諾されていないメディア，および，許諾されていない高品質での不正再生を防いでいる．

## 4 従来法との比較

ここでは，提案法の特徴について，従来法 [9, 10] と比較することによりまとめる．表 1 にそれぞれの方式の特徴を示す．同表より，管理鍵を一つとし，かつ，結託攻撃耐性を有しているという条件のもとで，従来法 [9] はある一つのメディアの一つの品質尺度にのみ，従来法 [10] は各メディアの一つの品質尺度にのみにそれぞれ階層構造を設定可能であるのに対して，提案法のみが各メディアの複数の品質尺度に対して階層構造を設定できる．また，従来法 [9] では，最高品質での再生を許諾されたユーザに管理鍵を配送しているのに対して，提案法では，安全性の観点から，いずれのユーザにも管理鍵を配送することはない．

## 5 あとがき

本稿では，再帰ハッシュ連鎖を用いたメディアコンテンツのアクセス制御のための多次元暗号鍵派生方式を提案した．提案法は，あるハッシュ連鎖からの出力値を別のハッシュ連鎖の入力値として利用する，再帰ハッシュ連鎖を用いて，制御対象となるメディアの個数，各メディアの品質尺度の種類，および，品質尺度の階層数に関わらず，管理鍵を常に一つとする．提案法は，品質尺度ごとに暗号鍵の独立性を保持することで，不正ユーザが互いの鍵を共有し，許諾されていない高品質でコンテンツの再生を企てる結託攻撃に対して耐性を考慮している．

今後の課題として，配送鍵の個数の削減手法やハッシュ演算処理の軽減について検討する．

## 謝辞

本研究は，研究費（23800010）の助成を受けたものである．

## 参考文献

[1] R. Grosbois, P. Gerbelot, and T. Ebrahimi, “Authentication and access control in the JPEG 2000 compressed domain, ” Proc. SPIE, vol.4472, pp.95–104, 2001.

[2] J.C. Birget, X. Zou, G. Noubir, and B. Ramamurthy: “Hierarchy-based access control in distributed environment,” Proc. IEEE Int’l Conf. Communications, vol.1, pp.229–233, 2001.

[3] L. Lamport, “Password authentication with insecure communication,” Communications of the ACM, vol.24, no.11, pp.770–772, 1981.

[4] Y. Wu, D. Ma, and R.H. Deng, “Progressive protection of JPEG 2000 codestreams,” Proc. IEEE Int’l Conf. Image Process., pp.3447–3450, Singapore, 2004.

[5] M. Joye and S. Yen, “One-way cross-trees and their applications,” Proc. IACR Int’l Conf. Practice and Theory PKC, pp.355–358, 2002.

[6] 須賀祐治, 岩村恵市: “DAG における鍵派生方式の枝切り改良方式,” 信学 SCIS, 2C2-4, 2005.

[7] M. Fujiyoshi, S. Imaizumi, and H. Kiya, “Encryption of composite multimedia contents for access control,” IEICE Trans. Fundamentals, vol.E90-A, no.3, pp.590–596, 2007.

[8] Y. G. Won, T. M. Bae, and Y. M. Ro, “Scalable protection and access control in full scalable video coding,” Proc. Int’l Workshop on Digital Watermarking, pp.407–421, 2006.

[9] S. Imaizumi, M. Fujiyoshi, and H. Kiya, “An efficient access control method for composite multimedia content,” IEICE Electronics Express,, vol.7, no.20, pp.1534–1538, 2010.

[10] S. Imaizumi, N. Aoki, H. Kobayashi, M. Fujiyoshi, and H. Kiya, “An efficient access control method for composite multimedia content,” Proc. Int’l Workshop on on Advanced Image Technology, 2012, to be published.