

【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21年12月10日 (2009.12.10)

【公開番号】特開2008-131078(P2008-131078A)

【公開日】平成20年6月5日 (2008.6.5)

【年通号数】公開・登録公報2008-022

【出願番号】特願2006-310213(P2006-310213)

【国際特許分類】

H 0 4 L 9/08 (2006.01)

【F I】

H 0 4 L 9/00 6 0 1 C

H 0 4 L 9/00 6 0 1 E

【手続補正書】

【提出日】平成21年10月23日 (2009.10.23)

【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】

複数の有向枝により構成される有向グラフで、当該有向グラフを構成する最大長の有向枝のひとつの始点が、当該有向グラフの始点と一致する有向グラフを取得する有向グラフ取得部と；

前記有向グラフ取得部により取得された前記有向グラフに基づいてコンテンツ又はコンテンツ鍵を暗号化又は復号するためのセット鍵を生成する鍵生成部と；

を備える、情報処理装置。

【請求項 2】

前記鍵生成部は、

前記有向グラフにおけるある座標点に対応する部分集合  $S$  の中間鍵  $t(S)$  の入力に応じて、当該座標点に対応する部分集合  $S$  に対応する前記セット鍵  $k(S)$  と、当該座標点  $S$  を始点とする前記有向枝の終点の座標点  $S_1, S_2, \dots, S_k$  の中間鍵  $t(S_1), t(S_2), \dots, t(S_k)$  と、を出力する、請求項 1 に記載の情報処理装置。

【請求項 3】

前記鍵生成部は、

前記有向グラフにおけるある座標点に対応する部分集合  $S$  のセット鍵  $k(S)$  の入力に応じて、当該座標点  $S$  を始点とする前記有向枝の終点の座標点  $S_1, S_2, \dots, S_k$  のセット鍵  $k(S_1), k(S_2), \dots, k(S_k)$  を出力する、請求項 1 に記載の情報処理装置。

【請求項 4】

さらに、前記セット鍵を用いてコンテンツ又はコンテンツ鍵を暗号化する暗号化部を備える、請求項 2 又は 3 に記載の情報処理装置。

【請求項 5】

所定の 2 分木構造を構成する葉ノード  $1 \sim n$  ( $n$  は自然数) の一部又は全部にそれぞれ対応付けられた端末装置に対し、前記暗号化部により暗号化された前記コンテンツ又は前記コンテンツ鍵を送信する送信部をさらに備える、請求項 4 に記載の情報処理装置。

【請求項 6】

前記葉ノード  $1 \sim n$  の部分集合を  $S_i$  と定義して、前記セット鍵又は前記コンテンツ鍵

で暗号化された前記コンテンツの復号を許可する前記端末装置の集合  $(N \setminus R)$  を決定し、前記集合  $(N \setminus R) = S_1 \cup S_2 \cup \dots \cup S_m$  を満たす  $m$  個の部分集合  $S_1 \sim S_m$  を決定する部分集合決定部をさらに備える、請求項 5 に記載の情報処理装置。

【請求項 7】

前記部分集合決定部は、

前記  $m$  が最小となるように、前記部分集合  $S_1 \sim S_m$  を決定する、請求項 6 に記載の情報処理装置。

【請求項 8】

前記送信部は、

前記集合  $(N \setminus R)$  を表す情報、又は、前記集合  $(N \setminus R)$  を構成する前記部分集合  $S_1 \sim S_m$  を表す情報を、前記端末装置に送信する、請求項 7 に記載の情報処理装置。

【請求項 9】

さらに、前記セット鍵を用いてコンテンツ又はコンテンツ鍵を復号する復号部を備える、請求項 1 に記載の情報処理装置。

【請求項 10】

所定の 2 分木構造を構成する葉ノード  $1 \sim n$  ( $n$  は自然数) の 1 つ以上に対応付けられ、前記セット鍵を用いて暗号化されたコンテンツ又はコンテンツ鍵を受信する受信部をさらに備える、請求項 9 に記載の情報処理装置。

【請求項 11】

前記受信部が受信する前記暗号化されたコンテンツ又はコンテンツ鍵は、前記葉ノード  $1 \sim n$  の部分集合として定義された集合  $S_i$  の中で、自身に対応付けられた前記葉ノードを含む集合  $S$  の要素である前記葉ノードに対応付けられた 1 つ以上の情報処理装置が復号可能である、請求項 10 に記載の情報処理装置。

【請求項 12】

複数の有向枝により構成される仮有向グラフに対し、当該仮有向グラフを構成する前記複数の有向枝の中から、より長い前記有向枝を残すことにより生成された有向グラフを取得する有向グラフ取得部と；

前記有向グラフ取得部により取得された前記有向グラフに基づいてコンテンツ又はコンテンツ鍵を暗号化又は復号するためのセット鍵を生成する鍵生成部と；  
を備える、情報処理装置。

【請求項 13】

番号  $1 \sim n$  ( $n$  は自然数) が対応付けられた  $n$  個の葉ノードと、根ノードと、前記根ノード及び前記葉ノード以外の複数の中間ノードと、から構成される 2 分木構造に対し、ある中間ノード  $v$  又は根ノード  $v$  の下位に配置された複数の前記葉ノードの中で左端に位置する前記葉ノードの番号が  $l_v$ 、そして右端に位置する前記葉ノードの番号が  $r_v$  と定義されており、

さらに、自然数  $i$  及び  $j$  ( $i < j$ ) に対して、集合  $(i \sim j)$  が  $\{\{i\}, \{i, i+1\}, \dots, \{i, i+1, \dots, j-1, j\}\}$  と表記され、集合  $(i \sim j)$  が  $\{\{j\}, \{j, j-1\}, \dots, \{j, j-1, \dots, i+1, i\}\}$  と表記されるものと仮定されており、

集合  $(1 \sim n)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に左から右に向かって包含関係が大きくなるように配列され、前記根ノードに対応付けられた第 1 水平座標軸が設定され、

また、集合  $(2 \sim n)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に右から左に向かって包含関係が大きくなるように配列され、前記根ノードに対応付けられた第 2 水平座標軸が設定されており、

さらに、前記中間ノードの各々について、

集合  $(l_v \sim r_v - 1)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に左から右に向かって包含関係が大きくなるように配列され、ある中間ノード  $v$  に対応付けられた第 3 水平座標軸が設定され、

また、集合  $(1v + 1 \dots rv)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に右から左に向かって包含関係が大きくなるように配列され、ある中間ノード  $v$  に対応付けられた第 4 水平座標軸が設定された上で、

所定の整数  $k$  に対し、 $n^{(x-1)/k} < (rv - 1v + 1) \cdot n^{x/k}$  を満たす自然数  $x$  に応じて長さ  $n^{i/k}$  ( $i = 0, 1, \dots, x-1$ ) を有する複数の有向枝を前記第 1 ~ 4 水平座標軸上に配置して形成された仮有向グラフを処理する情報処理装置であって、

前記仮有向グラフを取得する仮有向グラフ取得部と；

前記仮有向グラフ取得部により取得された前記仮有向グラフを構成する複数の有向枝の中から、より長い前記有向枝を残して有向グラフを生成する有向グラフ生成部と；

前記有向グラフに基づいてコンテンツ又はコンテンツ鍵を暗号化するためのセット鍵を生成する鍵生成部と；

を備える、情報処理装置。

#### 【請求項 14】

番号  $1 \sim n$  ( $n$  は自然数) が対応付けられた  $n$  個の葉ノードと、根ノードと、前記根ノード及び前記葉ノード以外の複数の中間ノードと、から構成される 2 分木構造を設定し、自然数  $i$  及び  $j$  ( $i < j$ ) に関して、集合  $(i \dots j)$  を  $\{\{i\}, \{i, i+1\}, \dots, \{i, i+1, \dots, j-1, j\}\}$ 、集合  $(i \dots j)$  を  $\{\{j\}, \{j, j-1\}, \dots, \{j, j-1, \dots, i+1, i\}\}$  と定義して、ある中間ノード  $v$  又は根ノード  $v$  の下位に配置された複数の前記葉ノードのうち、左端に位置する前記葉ノードの番号を  $1v$ 、右端に位置する前記葉ノードの番号を  $rv$  と設定する木構造設定部と；

集合  $(1 \dots n)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に左から右に向かって包含関係が大きくなるように配列された、前記根ノードに対応する第 1 水平座標軸と、

集合  $(2 \dots n)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に右から左に向かって包含関係が大きくなるように配列された、前記根ノードに対応する第 2 水平座標軸と、

前記中間ノードの各々について、

集合  $(1v \dots rv - 1)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に左から右に向かって包含関係が大きくなるように配列された、ある中間ノード  $v$  に対応する第 3 水平座標軸と、

集合  $(1v + 1 \dots rv)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に右から左に向かって包含関係が大きくなるように配列された、ある中間ノード  $v$  に対応する第 4 水平座標軸と、を設定し、

前記第 3 水平座標軸上の右端に位置する座標点の右側と、前記第 2 及び第 4 水平座標軸上の左端に位置する座標点の左側と、にそれぞれ 2 個の仮座標点を配置し、

前記第 1 水平座標軸上の右端に位置する座標点を第 1 の仮座標点として設定し、当該第 1 の仮座標点の右側に第 2 の仮座標点を配置する座標軸設定部と；

所定の整数  $k$  を設定し、

$n^{(x-1)/k} < (rv - 1v + 1) \cdot n^{x/k}$  を満たす整数  $x$  を算定した上で、

整数  $i = 0 \sim x-1$  の各々について、

$n^{i/k}$  の長さを有する右方向を向いた一又は複数の有向枝を連結して前記第 1 及び第 3 水平座標軸上の最左にある座標点を始点とする有向パスを形成し、

$n^{i/k}$  の長さを有する左方向を向いた一又は複数の有向枝を連結して前記第 2 及び第 4 水平座標軸上の最右にある座標点を始点とする有向パスを形成し、

前記第 1 ~ 4 水平座標軸の各々について、前記各仮座標点を始点又は終点とする全ての前記有向枝を除外し、

前記第 1 ~ 4 水平座標軸上の各座標点に到達する前記有向枝のうち、最長の有向枝以外の有向枝を除外することにより、

集合  $(1 \dots n - 1)$ 、集合  $(2 \dots n)$ 、集合  $(1v + 1 \dots rv)$ 、集合  $(1v \dots rv -$

1) に関する有向グラフをそれぞれ生成し、

前記集合  $(1 \sim n - 1)$  に関する有向グラフに対し、前記第 1 水平座標軸上にある前記第 1 の仮座標点を終点とする長さ 1 の有向枝を追加して、集合  $(1 \sim n)$  に関する有向グラフを生成する有向グラフ生成部と；

を備える、情報処理装置。

【請求項 15】

前記有向グラフに基づいて、コンテンツ又はコンテンツ鍵を暗号化するためのセット鍵を生成する鍵生成部を備え、

前記鍵生成部は、

前記有向グラフにおけるある座標点に対応する部分集合  $S$  の中間鍵  $t(S)$  の入力に応じて、当該座標点に対応する部分集合  $S$  に対応する前記セット鍵  $k(S)$  と、当該座標点  $S$  を始点とする前記有向枝の終点の座標点  $S_1, S_2, \dots, S_k$  の中間鍵  $t(S_1), t(S_2), \dots, t(S_k)$  と、を出力する、請求項 14 に記載の情報処理装置。

【請求項 16】

前記有向グラフに基づいて、コンテンツ又はコンテンツ鍵を暗号化するためのセット鍵を生成する鍵生成部を備え、

前記鍵生成部は、

前記有向グラフにおけるある座標点に対応する部分集合  $S$  のセット鍵  $k(S)$  の入力に応じて、当該座標点  $S$  を始点とする前記有向枝の終点の座標点  $S_1, S_2, \dots, S_k$  のセット鍵  $k(S_1), k(S_2), \dots, k(S_k)$  を出力する、請求項 14 に記載の情報処理装置。

【請求項 17】

有向グラフに基づいて、コンテンツ又はコンテンツ鍵を復号するためのセット鍵を生成する鍵生成部を備え、

前記有向グラフは、

番号  $1 \sim n$  ( $n$  は自然数) が対応付けられた  $n$  個の葉ノードと、根ノードと、前記根ノード及び前記葉ノード以外の複数の中間ノードと、から構成される 2 分木構造を設定し、自然数  $i$  及び  $j$  ( $i < j$ ) に関して、集合  $(i \sim j)$  を  $\{\{i\}, \{i, i+1\}, \dots, \{i, i+1, \dots, j-1, j\}\}$ 、集合  $(i \sim j)$  を  $\{\{j\}, \{j, j-1\}, \dots, \{j, j-1, \dots, i+1, i\}\}$  と定義して、ある中間ノード  $v$  又は根ノード  $v$  の下位に配置された複数の前記葉ノードのうち、左端に位置する前記葉ノードの番号を  $lv$ 、右端に位置する前記葉ノードの番号を  $rv$  と設定し、

集合  $(1 \sim n)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に左から右に向かって包含関係が大きくなるように配列された、前記根ノードに対応する第 1 水平座標軸と、

集合  $(2 \sim n)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に右から左に向かって包含関係が大きくなるように配列された、前記根ノードに対応する第 2 水平座標軸と、

前記中間ノードの各々について、

集合  $(lv \sim rv - 1)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に左から右に向かって包含関係が大きくなるように配列された、ある中間ノード  $v$  に対応する第 3 水平座標軸と、

集合  $(lv + 1 \sim rv)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に右から左に向かって包含関係が大きくなるように配列された、ある中間ノード  $v$  に対応する第 4 水平座標軸と、を設定し、

前記第 3 水平座標軸上の右端に位置する座標点の右側と、前記第 2 及び第 4 水平座標軸上の左端に位置する座標点の左側と、にそれぞれ 2 個の仮座標点を配置し、

前記第 1 水平座標軸上の右端に位置する座標点を第 1 の仮座標点として設定し、当該第 1 の仮座標点の右側に第 2 の仮座標点を配置し、

所定の整数  $k$  を設定し、

$n(x-1)/k < (rv - lv + 1) \quad n^{x/k}$  を満たす整数  $x$  を算定した上で、  
整数  $i = 0 \sim x - 1$  の各々について、

$n^{i/k}$  の長さを有する右方向を向いた一又は複数の有向枝を連結して前記第 1 及び第 3 水平座標軸上の最左にある座標点を始点とする有向パスを形成し、

$n^{i/k}$  の長さを有する左方向を向いた一又は複数の有向枝を連結して前記第 2 及び第 4 水平座標軸上の最右にある座標点を始点とする有向パスを形成し、

前記第 1 ~ 4 水平座標軸の各々について、前記各仮座標点を始点又は終点とする全ての前記有向枝を除外し、

前記第 1 ~ 4 水平座標軸上の各座標点に到達する前記有向枝のうち、最長の有向枝以外の有向枝を除外することにより、

集合  $(1 \quad n - 1)$ 、集合  $(2 \quad n)$ 、集合  $(lv + 1 \quad rv)$ 、集合  $(lv \quad rv - 1)$  に関する有向グラフをそれぞれ生成し、

前記集合  $(1 \quad n - 1)$  に関する有向グラフに対し、前記第 1 水平座標軸上にある前記第 1 の仮座標点を終点とする長さ 1 の有向枝を追加して、集合  $(1 \quad n)$  に関する有向グラフを生成することにより得られる、端末装置。

#### 【請求項 18】

複数の有向枝により構成される仮有向グラフに対し、当該仮有向グラフを構成する前記複数の有向枝の中から、より長い前記有向枝を残すことにより生成された有向グラフを取得する有向グラフ取得ステップと；

前記有向グラフ取得部により取得された前記有向グラフに基づいてコンテンツ又はコンテンツ鍵を暗号化又は復号するためのセット鍵を生成する鍵生成ステップと；  
を含む、情報処理方法。

#### 【請求項 19】

番号  $1 \sim n$  ( $n$  は自然数) が対応付けられた  $n$  個の葉ノードと、根ノードと、前記根ノード及び前記葉ノード以外の複数の中間ノードと、から構成される 2 分木構造に対し、ある中間ノード  $v$  又は根ノード  $v$  の下位に配置された複数の前記葉ノードの中で左端に位置する前記葉ノードの番号が  $lv$ 、そして右端に位置する前記葉ノードの番号が  $rv$  と定義されており、

さらに、自然数  $i$  及び  $j$  ( $i < j$ ) に対して、集合  $(i \quad j)$  が  $\{\{i\}, \{i, i + 1\}, \dots, \{i, i + 1, \dots, j - 1, j\}\}$  と表記され、集合  $(i \quad j)$  が  $\{\{j\}, \{j, j - 1\}, \dots, \{j, j - 1, \dots, i + 1, i\}\}$  と表記されるものと仮定されており、

集合  $(1 \quad n)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に左から右に向かって包含関係が大きくなるように配列され、前記根ノードに対応付けられた第 1 水平座標軸が設定され、

また、集合  $(2 \quad n)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に右から左に向かって包含関係が大きくなるように配列され、前記根ノードに対応付けられた第 2 水平座標軸が設定されており、

さらに、前記中間ノードの各々について、

集合  $(lv \quad rv - 1)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に左から右に向かって包含関係が大きくなるように配列され、ある中間ノード  $v$  に対応付けられた第 3 水平座標軸が設定され、

また、集合  $(lv + 1 \quad rv)$  に含まれる各部分集合に対応付けられた座標点が水平座標軸上に右から左に向かって包含関係が大きくなるように配列され、ある中間ノード  $v$  に対応付けられた第 4 水平座標軸が設定された上で、

所定の整数  $k$  に対し、 $n(x-1)/k < (rv - lv + 1) \quad n^{x/k}$  を満たす自然数  $x$  に応じて長さ  $n^{i/k}$  ( $i = 0, 1, \dots, x - 1$ ) を有する複数の有向枝を前記第 1 ~ 4 水平座標軸上に配置して形成された仮有向グラフを処理する情報処理方法であって、

前記仮有向グラフを取得する仮有向グラフ取得ステップと；

前記仮有向グラフ取得部により取得された前記仮有向グラフを構成する複数の有向枝の中から、より長い前記有向枝を残して有向グラフを生成する有向グラフ生成ステップと；

前記有向グラフに基づいてコンテンツ又はコンテンツ鍵を暗号化するためのセット鍵を生成する鍵生成ステップと；

を含む、情報処理方法。

【請求項 20】

番号  $1 \sim n$  ( $n$  は自然数) が対応付けられた  $n$  個の葉ノードと、根ノードと、前記根ノード及び前記葉ノード以外の複数の中間ノードと、から構成される 2 分木構造を設定し、自然数  $i$  及び  $j$  ( $i < j$ ) に関して、集合  $(i \sim j)$  を  $\{\{i\}, \{i, i+1\}, \dots, \{i, i+1, \dots, j-1, j\}\}$ 、集合  $(i \sim j)$  を  $\{\{j\}, \{j, j-1\}, \dots, \{j, j-1, \dots, i+1, i\}\}$  と定義して、ある中間ノード  $v$  又は根ノード  $v$  の下位に配置された複数の前記葉ノードのうち、左端に位置する前記葉ノードの番号を  $lv$ 、右端に位置する前記葉ノードの番号を  $rv$  と設定する木構造設定ステップと；

集合  $(1 \sim n)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に左から右に向かって包含関係が大きくなるように配列された、前記根ノードに対応する第 1 水平座標軸と、

集合  $(2 \sim n)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に右から左に向かって包含関係が大きくなるように配列された、前記根ノードに対応する第 2 水平座標軸と、

前記中間ノードの各々について、

集合  $(lv \sim rv - 1)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に左から右に向かって包含関係が大きくなるように配列された、ある中間ノード  $v$  に対応する第 3 水平座標軸と、

集合  $(lv + 1 \sim rv)$  に含まれる各部分集合に対応付けられた座標点が、水平座標軸上に右から左に向かって包含関係が大きくなるように配列された、ある中間ノード  $v$  に対応する第 4 水平座標軸と、を設定し、

前記第 3 水平座標軸上の右端に位置する座標点の右側と、前記第 2 及び第 4 水平座標軸上の左端に位置する座標点の左側と、にそれぞれ 2 個の仮座標点を配置し、

前記第 1 水平座標軸上の右端に位置する座標点を第 1 の仮座標点として設定し、当該第 1 の仮座標点の右側に第 2 の仮座標点を配置する座標軸設定ステップと；

所定の整数  $k$  を設定し、

$n^{(x-1)/k} < (rv - lv + 1) \leq n^{x/k}$  を満たす整数  $x$  を算定した上で、

整数  $i = 0 \sim x - 1$  の各々について、

$n^{i/k}$  の長さを有する右方向を向いた一又は複数の有向枝を連結して前記第 1 及び第 3 水平座標軸上の最左にある座標点を始点とする有向パスを形成し、

$n^{i/k}$  の長さを有する左方向を向いた一又は複数の有向枝を連結して前記第 2 及び第 4 水平座標軸上の最右にある座標点を始点とする有向パスを形成し、

前記第 1 ～ 4 水平座標軸の各々について、前記各仮座標点を始点又は終点とする全ての前記有向枝を除外し、

前記第 1 ～ 4 水平座標軸上の各座標点に到達する前記有向枝のうち、最長の有向枝以外の有向枝を除外することにより、

集合  $(1 \sim n - 1)$ 、集合  $(2 \sim n)$ 、集合  $(lv + 1 \sim rv)$ 、集合  $(lv \sim rv - 1)$  に関する有向グラフをそれぞれ生成し、

前記集合  $(1 \sim n - 1)$  に関する有向グラフに対し、前記第 1 水平座標軸上にある前記第 1 の仮座標点を終点とする長さ 1 の有向枝を追加して、集合  $(1 \sim n)$  に関する有向グラフを生成する有向グラフ生成ステップと；

を含む、情報処理方法。