【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2008-131072(P2008-131072A)
【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2006-310182(P2006-310182)
【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仮有向グラフに対し、当該仮有向グラフを構成する少なくとも１つの前記有向枝をより短い有向枝に置換する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また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】
前記有向グラフは，前記仮有向グラフを構成する前記複数の有向枝の中で，前記連続する有向枝の最大数を超えないように、前記仮有向グラフを構成する少なくとも１つの有向枝をより短い有向枝に置換して生成される、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Ｓ１，Ｓ２，・・・，Ｓｋの中間鍵ｔ（Ｓ１），ｔ（Ｓ２），・・・，ｔ（Ｓｋ）と、を出力する、請求項２に記載の情報処理装置。
【請求項４】
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Ｓ１，Ｓ２，・・・，Ｓｋのセット鍵ｋ（Ｓ１），ｋ（Ｓ２），・・・，ｋ（Ｓｋ）を出力する、請求項２に記載の情報処理装置。
【請求項５】
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３又は４に記載の情報処理装置。
【請求項６】
所定の２分木構造を構成する葉ノード１～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５に記載の情報処理装置。
【請求項７】
前記葉ノード１～ｎの部分集合をＳｉ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＼Ｒ）を決定し、前記集合（Ｎ＼Ｒ）＝Ｓ１∪Ｓ２∪・・・∪Ｓｍを満たすｍ個の部分集合Ｓ１～Ｓｍを決定する部分集合決定部をさらに備える、請求項６に記載の情報処理装置。
【請求項８】
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Ｓ１～Ｓｍを決定する、請求項７に記載の情報処理装置。
【請求項９】
前記集合（Ｎ＼Ｒ）を表す情報、又は、前記集合（Ｎ＼Ｒ）を構成する前記部分集合Ｓ１～Ｓｍを表す情報を、前記端末装置に送信する送信部をさらに備える、請求項８に記載の情報処理装置。
【請求項１０】
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１１】
所定の２分木構造を構成する葉ノード１～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、
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～ｎの部分集合として定義された集合Ｓｉ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】
前記有向グラフ取得部は、
連続する前記有向枝により構成される各有向パスの終点方向に向かって、より短い有向枝が配置されるように置換された前記有向グラフを取得する、請求項１に記載の情報処理装置。
【請求項１３】
番号１～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→ｊ）が｛｛ｉ｝，｛ｉ，ｉ＋１｝，．．．，｛ｉ，ｉ＋１，．．．，ｊ－１，ｊ｝｝と表記され、集合（ｉ←ｊ）が｛｛ｊ｝，｛ｊ，ｊ－１｝，．．．，｛ｊ，ｊ－１，．．．，ｉ＋１，ｉ｝｝と表記されるものと仮定されており，
集合（１→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←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→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、
　そして集合（ｌｖ＋１←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，$n^{(x-1)/k}<(rv-lv+1)\leqq n^{x/k}$を満たす自然数ｘに応じて長さ$n^{i/k}$（ｉ＝０，１，．．．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構成する少なくとも１つの前記有向枝をより短い有向枝に置換して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が取得し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１４】
　番号１～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→ｊ）を｛｛ｉ｝，｛ｉ，ｉ＋１｝，．．．，｛ｉ，ｉ＋１，．．．，ｊ－１，ｊ｝｝、集合（ｉ←ｊ）を｛｛ｊ｝，｛ｊ，ｊ－１｝，．．．，｛ｊ，ｊ－１，．．．，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部と；
　集合（１→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←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→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←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１～４水平座標軸上の左端に位置する座標点の左側と、前記第２～４水平座標軸上の右端に位置する座標点の右側と、にそれぞれ１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仮座標点として設定する座標軸設定部と；
　所定の整数ｋを設定し、
　$n^{(x-1)/k}<(rv-lv+1)\leqq n^{x/k}$を満たす自然数ｘを算定した上で、
　整数ｉ＝０～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→ｎ－１）、集合（２←ｎ）、集合（ｌｖ＋１←ｒｖ）、集合（ｌｖ→ｒｖ－１）に関する仮有向グラフをそれぞれ生成し、
　集合（１→ｎ－１）に関する仮有向グラフに対し、前記第１水平座標軸上の右端に位置

する座標点を終点とする長さ１の有向枝を追加して、集合（１→ｎ）に関する仮有向グラフを生成する仮有向グラフ生成部と；
残存する前記有向枝をより短い有向枝に置換して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る、請求項１４に記載の情報処理装置。
【請求項１６】
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Ｓ１，Ｓ２，・・・，Ｓｋの中間鍵ｔ（Ｓ１），ｔ（Ｓ２），・・・，ｔ（Ｓｋ）と、を出力する、請求項１５に記載の情報処理装置。
【請求項１７】
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Ｓ１，Ｓ２，・・・，Ｓｋのセット鍵ｋ（Ｓ１），ｋ（Ｓ２），・・・，ｋ（Ｓｋ）を出力する、請求項１５に記載の情報処理装置。
【請求項１８】
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～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→ｊ）を｛｛ｉ｝，｛ｉ，ｉ＋１｝，．．．，｛ｉ，ｉ＋１，．．．，ｊ－１，ｊ｝｝、集合（ｉ←ｊ）を｛｛ｊ｝，｛ｊ，ｊ－１｝，．．．，｛ｊ，ｊ－１，．．．，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→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←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→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←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１～４水平座標軸上の左端に位置する座標点の左側と、前記第２～４水平座標軸上の右端に位置する座標点の右側と、にそれぞれ１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仮座標点として設定し、
所定の整数ｋを設定し、
$n^{(x-1)/k} < (rv - lv + 1) \leqq n^{x/k}$ を満たす自然数ｘを算定した上で、
整数ｉ＝０～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→ｎ－１）、集合（２←ｎ）、集合（ｌｖ＋１←ｒｖ）、集合（ｌｖ→ｒｖ－１）に関する仮有向グラフをそれぞれ生成し、
集合（１→ｎ－１）に関する仮有向グラフに対し、前記第１水平座標軸上の右端に位置する座標点を終点とする長さ１の有向枝を追加して、集合（１→ｎ）に関する仮有向グラフを生成し、
残存する前記有向枝によって形成された有向パスの中から、前記有向パスを構成する有向枝数が最大となる最長の有向パスを決定し、
前記各有向パスの有向枝数が、前記最長の有向パスの有向枝数を超えないように、前記各有向パスを構成する有向枝を、より短い有向枝に置換することによって得られる、端末装置。
【請求項１９】
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少なくとも１つの前記有向枝をより短い有向枝に置換する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また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２０】
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ステップを含み、
前記有向グラフは、
番号１～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→ｊ）を｛｛ｉ｝，｛ｉ，ｉ＋１｝，．．．，｛ｉ，ｉ＋１，．．．，ｊ－１，ｊ｝｝、集合（ｉ←ｊ）を｛｛ｊ｝，｛ｊ，ｊ－１｝，．．．，｛ｊ，ｊ－１，．．．，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→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←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→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←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１～４水平座標軸上の左端に位置する座標点の左側と、前記第２～４水平座標軸

上の右端に位置する座標点の右側と、にそれぞれ１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仮座標点として設定し、

所定の整数ｋを設定し、

$n^{(x-1)/k} < (rv - lv + 1) \leqq n^{x/k}$を満たす自然数ｘを算定した上で、

整数ｉ＝０～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→ｎ－１）、集合（２←ｎ）、集合（ｌｖ＋１←ｒｖ）、集合（ｌｖ→ｒｖ－１）に関する仮有向グラフをそれぞれ生成し、

集合（１→ｎ－１）に関する仮有向グラフに対し、前記第１水平座標軸上の右端に位置する座標点を終点とする長さ１の有向枝を追加して、集合（１→ｎ）に関する仮有向グラフを生成し、

残存する前記有向枝によって形成された有向パスの中から、前記有向パスを構成する有向枝数が最大となる最長の有向パスを決定し、

前記各有向パスの有向枝数が、前記最長の有向パスの有向枝数を超えないように、前記各有向パスを構成する有向枝を、より短い有向枝に置換することによって得られることを特徴とする、鍵生成方法。