

【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22年6月24日(2010.6.24)

【公表番号】特表2008-537433(P2008-537433A)
 【公表日】平成20年9月11日(2008.9.11)
 【年通号数】公開・登録公報2008-036
 【出願番号】特願2008-507543(P2008-507543)
 【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 B

H 0 4 L 9/00 6 0 1 E

【手続補正書】

【提出日】平成22年3月19日(2010.3.19)

【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】

所定数のノードからなる複数のノード群を含む層構造のブロードキャスト暗号化(broadcast encryption:BE)システムに用いられるタグの形成方法において、

(a) 除かれた少なくとも一つの葉ノード(leaf node)を検出するステップと、

(b) 第 0 の層を構成するノード ID (identification) が与えられた複数のノードのうち、前記除かれた少なくとも一つの葉ノードが従属する少なくとも一つのノードに与えられた前記ノード ID を前記除かれた少なくとも一つの葉ノードの第 0 の層におけるノードパス(node path) ID に設定するステップと、

(c) 対応する前記葉ノードのノード ID が増加する順番に少なくとも一つのノードパス ID の連結によって前記第 0 の層についてのタグリストを形成するステップと、

(d) 前記 (b) ステップ及び前記 (c) ステップを最後の層まで繰り返し行い、前記最後の層についてのタグリストまで形成するステップとを有することを特徴とするブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 2】

前記各ノードパス ID には、各ノードパス ID に相当するノードの親(parent)ノードの情報を示す群(group) ID が結合されることを特徴とする請求項 1 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 3】

各レベルの層における最初のノードパス ID には、群 ID として「0」を結合することを特徴とする請求項 2 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 4】

各レベルの層における 2 番目のノードパス ID が以前のノードパス ID と同じノード群内にある場合には、以前のノードパス ID に結合された群 ID と同じ群 ID が結合されることを特徴とする請求項 3 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 5】

各レベルの層における 2 番目のノードパス ID が以前のノードパス ID とは異なるノード群内にある場合には、以前のノードパス ID に「1」を加えた後に「2」で割った余り値である群 ID が結合されることを特徴とする請求項 3 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 6】

前記各ノードパス ID は、前記各ノードパス ID に相当するノードの親ノードの群 ID を結合することを特徴とする請求項 1 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 7】

前記ノード ID は、16 進数により与えられ、前記ノード群はそれぞれ 16 個のノードからなることを特徴とする請求項 1 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 8】

前記最後の層は、第 15 の層であることを特徴とする請求項 1 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 9】

ツリートポロジ (tree topology) 構造内の特定のノードからの下位の枝 (branches) の全ての葉ノードが除かれた場合に、前記除かれた下位の枝の全ての葉ノードの前記各ノードパス ID は各ノードパス ID のうち最も小さなノードパス ID に置き換えられることを特徴とする請求項 2 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 10】

前記置き換えられた最も小さなノードパス ID は、所定数の「1」が連続する 2 進数の群 ID が結合されることを特徴とする請求項 9 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 11】

前記所定数は、前記ノードパス ID に相当するノードが構成するノード群内のノードの数の底が 2 の対数値であることを特徴とする請求項 10 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 12】

前記少なくとも一つの葉ノードに対して各層におけるノードパス ID を連結したものを前記少なくとも一つの葉ノードのノード ID とすることを特徴とする請求項 10 に記載のブロードキャスト暗号化システムにおけるタグの形成方法。

【請求項 13】

除かれた葉ノードの親ノードの ID を把握するステップと、
前記親ノードの ID 及び除かれた葉ノードの ID を順次に並べて、除かれたノードのリストを生成するステップと、
を含むことを特徴とする除かれたノードリストの生成方法。

【請求項 14】

前記生成ステップは、
0) 除かれた葉ノードに対する第 0 の層の親ノードの ID、
1) 前記除かれた葉ノードに対する第 1 の層の親ノードの ID、
2) 前記除かれた葉ノードに対する第 2 の層の親ノードの ID、
乃至、
n-2) 前記除かれた葉ノードに対する第 n-2 の層の親ノードの ID、及び
n-1) 第 n-1 の層に従属された前記除かれた葉ノードの ID、
を結合して、前記除かれたノードのリストを生成することを特徴とする請求項 13 に記載の除かれたノードリストの生成方法。

【請求項 15】

前記ノードはグループ化され、

前記 I D は、「ノードが従属するグループにおける前記ノードの順番に従って決定されるノードパス I D (Node Path Identification)」及び「前記ノードが従属するグループを示すグループ I D (Group Identification)」が結合されたことを特徴とする請求項 14 に記載の除かれたノードリストの生成方法。

【請求項 16】

前記グループ I D は、

各層における最初のノードに対しては第 1 の値で割当てられ、

各層における 2 番目からのノードに対しては、以前のノードと同じグループに従属すると前記第 1 の値で割当てられ、以前のノードと異なるグループに従属すると第 2 の値で割当てられることを特徴とする請求項 15 に記載の除かれたノードリストの生成方法。

【請求項 17】

前記第 2 の値は、

前記第 1 の値に「1」を加えた後に「2」で割った余り値であることを特徴とする請求項 16 に記載の除かれたノードリストの生成方法。

【請求項 18】

前記各層における最初のノードが、子ノードが全て除かれたノードであり、親ノードの子ノードが全て除かれたノードではないノードの子ノードであると、前記グループ I D は第 3 の値で割当てられることを特徴とする請求項 16 に記載の除かれたノードリストの生成方法。

【請求項 19】

前記各層における 2 番目からのノードが、子ノードが全て除かれたノードであり、親ノードの子ノードが全て除かれたノードではないノードの子ノードであると、前記グループ I D は前記第 3 の値で割当てられることを特徴とする請求項 16 に記載の除かれたノードリストの生成方法。

【請求項 20】

除かれた第 1 の葉ノードの親ノードである第 1 の親ノードの I D を把握するステップと、

前記第 1 の親ノードの I D 及び前記第 1 の葉ノードの I D を並べて生成される I D が、除かれたノード I D で収録されるリストを生成するステップと、
を含むことを特徴とする除かれたノードリストの生成方法。

【請求項 21】

前記ノードは、第 0 の層ないし第 $n-1$ の層に階層化され、

前記第 1 の葉ノードは、前記第 $n-1$ の層に従属され、

前記第 1 の親ノードの I D は、

「第 0 の層に従属する第 1 の親ノードの I D」、「第 1 の層に従属する第 1 の親ノードの I D」、乃至、「第 $n-2$ の層に従属する第 1 の親ノードの I D」を含むことを特徴とする請求項 20 に記載の除かれたノードリストの生成方法。

【請求項 22】

前記ノードはグループ化され、

前記 I D は、「ノードが従属するグループにおける前記ノードの順番に従って決定されるノードパス I D (Node Path Identification)」を含むことを特徴とする請求項 20 に記載の除かれたノードリストの生成方法。

【請求項 23】

除かれた第 2 の葉ノードの親ノードである第 2 の親ノードの I D を把握するステップを更に含み、

前記生成ステップは、

前記第 1 の親ノードの I D 及び前記第 1 の葉ノードの I D を並べて生成される I D が、除かれた第 1 の葉ノードの I D で収録され、前記第 2 の親ノードの I D 及び前記第 2 の葉

ノードの ID を並べて生成される ID が、除かれた第 2 の葉ノードの ID で収録されるリストを生成することを特徴とする請求項 20 に記載の除かれたノードリストの生成方法。

【請求項 24】

前記ノードは、第 0 の層ないし第 $n-1$ の層に階層化され、

前記第 1 の葉ノード及び前記第 2 の葉ノードは、前記第 $n-1$ の層に従属され、

前記生成ステップは、

「第 0 の層に従属する第 1 の親ノードの ID」、「第 0 の層に従属する第 2 の親ノードの ID」、「第 1 の層に従属する第 1 の親ノードの ID」、「第 1 の層に従属する第 2 の親ノードの ID」、乃至、「第 $n-2$ の層に従属する第 1 の親ノードの ID」、「第 $n-2$ の層に従属する第 2 の親ノードの ID」、前記第 1 の葉ノードの ID 及び前記第 2 の葉ノードの ID を並べて、前記除かれたノードのリストを生成することを特徴とする請求項 23 に記載の除かれたノードリストの生成方法。

【請求項 25】

前記ノードはグループ化され、

前記 ID は、「ノードが従属するグループにおける前記ノードの順番に従って決定されるノードパス ID (Node Path Identification)」及び「前記ノードが従属するグループを示すグループ ID (Group Identification)」が結合されたことを特徴とする請求項 24 に記載の除かれたノードリストの生成方法。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】ブロードキャスト暗号化システムにおけるタグの形成方法および除かれたノードリストの生成方法

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正の内容】

【0001】

本発明は、ブロードキャスト暗号化システムにおけるタグの形成方法および除かれたノードリストの生成方法に係り、さらに詳しくは、タグサイズの減少のための効率よい、ブロードキャスト暗号化システムにおけるタグの形成方法および除かれたノードリストの生成方法に関する。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正の内容】

【0016】

そこで、本発明の目的は、タグサイズの減少のために除かれた葉ノードのノード ID の効率よい配置を用いるブロードキャスト暗号化システムにおけるタグの形成方法および除かれたノードリストの生成方法を提供するところにある。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正の内容】

【0018】

好ましくは、前記各ノードパスIDには、各ノードパスIDに相当するノードの親ノードの情報を示す群IDが結合される。

好ましくは、各レベルの層における最初のノードパスIDには、群IDとして「0」を結合する。

好ましくは、各レベルの層における2番目のノードパスIDが以前のノードパスIDと同じノード群内にある場合には、以前のノードパスIDに結合された群IDと同じ群IDが結合される。

好ましくは、各レベルの層における2番目からのノードパスIDが以前のノードパスIDとは異なるノード群内にある場合には、以前のノードパスIDに「1」を加えた後に2で割った余り値である群IDが結合される。

好ましくは、前記各ノードパスIDは、前記各ノードパスIDに相当するノードの親ノードの群IDを結合する。

好ましくは、前記ノードIDは16進数により与えられ、前記ノード群はそれぞれ16個のノードからなる。

好ましくは、前記最後の層は、第15の層である。

好ましくは、前記ツリートポロジ構造内の特定のノードからの下位の枝(branches)の全ての葉ノードが除かれた場合に、前記除かれた下位の枝の全ての葉ノードの前記各ノードパスIDは各ノードパスIDのうち最も小さなノードパスIDに置き換えられる。

好ましくは、前記置き換えられた最も小さなノードパスIDは、所定数の「1」が連続する2進数の群IDが結合される。

好ましくは、前記所定数は、前記ノードパスIDに相当するノードが構成するノード群内のノードの数の底が2の対数値である。

好ましくは、前記少なくとも一つの葉ノードに対して前記各層におけるノードパスIDを連結したものを前記少なくとも一つの葉ノードのノードIDとする。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】変更

【補正の内容】

【0019】

上記目的を達成するために、本発明による除かれたノードリストの生成方法は、除かれた葉ノードの親ノードのIDを把握するステップと、前記親ノードのID及び除かれた葉ノードのIDを順次に並べて、除かれたノードのリストを生成するステップとを含むことを特徴とする。