【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10月22日(2009.10.22)

【公開番号】特開2008-113201(P2008-113201A)
【公開日】平成20年5月15日(2008.5.15)
【年通号数】公開・登録公報2008-019
【出願番号】特願2006-294639(P2006-294639)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ

【手続補正書】
【提出日】平成21年9月8日(2009.9.8)
【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】
ｎ個の受信装置がリーフに割り当てられ、高さが（$\log_Y n$）で表されるＹ分木構造を階層的に構成し、前記リーフとルートとの間に存在する中間ノードの下位に存在する複数の前記リーフからなるサブグループを構成する、木構造構成部と、
前記リーフおよび前記中間ノードそれぞれに対して、リーフキーg_yを割り当てるリーフキー割当部と、
前記中間ノードおよび前記ルートに、相異なるパラメータ$\nu_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とノードパラメータ$\gamma_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とをそれぞれ割り当てるパラメータ割当部と、
前記ルートから前記リーフに至るパスを特定し、当該パス上に存在する前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yと、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\nu_{x,y}$および前記ノードパラメータ$\gamma_{x,y}$に基づいて、鍵を算出する鍵算出部と、
を備える、鍵生成装置。
【請求項２】
前記鍵生成装置は、前記鍵算出部により算出された前記パス上の鍵セットを各受信装置それぞれに配布する配布部を、更に備える、請求項１に記載の鍵生成装置。
【請求項３】
前記鍵生成装置は、
素数ｐを無作為に選択し、前記素数ｐを位数とする双線形群Ｇを決定し、前記Ｇの生成元であるｇを無作為に選択し、秘密の乱数α（αは整数）を無作為に選択する乱数決定部を更に備え、
前記リーフキー割当部は、以下の式Ａを満たす前記リーフキーg_yを算出する、請求項１に記載の鍵生成装置。
【数１】

$$g_y = g^{(\alpha)^y} \quad \cdots(\text{式A})$$

（ｙ＝１，２，・・・，Ｙ，Ｙ＋２，・・・，２Ｙ）

【請求項４】
前記パラメータ割当部は、前記リーフを除く全てのノードと前記ルートのそれぞれに対して、ノードパラメータ$\gamma_{x,y}$（$\gamma_{x,y}$は整数）を無作為に選択し、以下の式Ｂで表されるパラメータ$\nu_{x,y}$を算出する、請求項３に記載の鍵生成装置。
【数２】

$$\nu_{x,y} = g^{(\gamma_{x,y})} \quad \cdots(式B)$$

【請求項５】
前記鍵算出部は、前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yの、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\gamma_{x,y}$乗で得られる値を、秘密鍵とし、
前記配布部は、前記鍵算出部において算出された秘密鍵を各受信装置に送信する送信部を更に備える、請求項４に記載の鍵生成装置。
【請求項６】
前記鍵算出部は、前記リーフキーg_yおよび前記パラメータ$\nu_{x,y}$に基づき、公開鍵を算出し、
前記配布部は、前記公開鍵を公開する公開鍵公開部を備える、請求項５に記載の鍵生成装置。
【請求項７】
ｎ個の受信装置のなかから排除する受信装置を特定し、排除されていない受信装置の集合Ｓを決定する、排除受信装置特定部を備える、暗号化装置。
【請求項８】
前記暗号化装置は、
整数ｔを無作為に選択し、セッション鍵$s = e(g_Y, g_1)^t$を決定するセッション鍵決定部と、
前記セッション鍵ｓを用いて、配信するコンテンツを暗号化する暗号化部と、
を更に備える、請求項７に記載の暗号化装置。
ここで、前記$e(g_Y, g_1)$は、双線形群上の２つの元g_Y、g_1に対する双線形写像を表す。
【請求項９】
前記セッション鍵決定部は、階層化された木構造において、前記排除された受信装置が割り当てられたリーフから前記ルートに至るパス上に存在する全てのノードそれぞれにマークをし、前記マークされたノードに割り当てられた前記パラメータ$\nu_{x,y}$と、前記マークされたノードを親ノードとする中間ノードに割り当てられた前記リーフキーg_yと、に基づいて、以下の式Ｃで表される$c_{x,y}$を算出するヘッダ要素算出部を、更に備える、請求項８に記載の暗号化装置。
【数３】

$$c_{x,y} = \left(\nu_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j}\right)^t \quad \cdots(式C)$$

ここで、$S_{x,y}$は、前記マークされたノードを親ノードとする各サブグループに所属する、マークされていない子ノードの集合を示す。
【請求項１０】
前記セッション鍵決定部は、前記ヘッダ要素算出部において得られた前記$c_{x,y}$と、g^tと、をヘッダ情報とするヘッダ情報生成部を更に備える、請求項９に記載の暗号化装置。
【請求項１１】
鍵生成装置および暗号化装置と通信可能な受信装置であって、

前記鍵生成装置において、ｎ個の受信装置がリーフに割り当てられ、高さが（$\log_Y n$）で表されるＹ分木構造を階層的に構成し、前記リーフとルートとの間に存在する中間ノードの下位に存在する複数の前記リーフからなるサブグループを構成し、前記リーフおよび前記中間ノードそれぞれに対して、リーフキーg_yを割り当て、前記中間ノードおよび前記ルートに、相異なるパラメータ$\nu_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とノードパラメータ$\gamma_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とをそれぞれ割り当て、前記ルートから前記リーフに至るパスを特定し、当該パス上に存在する前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yと、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\nu_{x,y}$および前記ノードパラメータ$\gamma_{x,y}$に基づいて算出された鍵を受信する、受信部を備える、受信装置。

【請求項１２】

前記受信装置は、暗号化コンテンツをセッション鍵ｓにより復号する復号部を更に備える、請求項１１に記載の受信装置。

【請求項１３】

前記受信部は、排除する受信装置が特定された情報である、排除されていない受信装置の集合Ｓに関する情報を更に受信し、

前記受信装置は、受信装置が前記集合Ｓに含まれているか否かを判定する判定部を更に備える、請求項１２に記載の受信装置。

【請求項１４】

前記判定部において、受信装置が前記集合Ｓに含まれていると判定された場合、前記復号部は、セッション鍵ｓを以下に示す式Ｄに基づいて算出し、算出された当該セッション鍵ｓを用いることで、前記暗号化コンテンツを復号化する、請求項１２に記載の受信装置。

【数４】

$$s=\frac{e(g_{i_{x'}},c_{x,y})}{e(g_{i_{x'}}^{\gamma_{i_{x'}-1}}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y+1-j+i_{x'}},g^t)}\quad\cdots(式D)$$

【請求項１５】

ｎ個の受信装置がリーフに割り当てられ、高さが（$\log_Y n$）で表されるＹ分木構造を階層的に構成し、前記リーフとルートとの間に存在する中間ノードの下位に存在する複数の前記リーフからなるサブグループを構成する木構造構成ステップと、

前記リーフおよび前記中間ノードそれぞれに対して、リーフキーg_yを割り当てるリーフキー割当ステップと、

前記中間ノードおよび前記ルートに、相異なるパラメータ$\nu_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とノードパラメータ$\gamma_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とをそれぞれ割り当てるパラメータ割当ステップと、

前記ルートから前記リーフに至るパスを特定し、当該パス上に存在する前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yと、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\nu_{x,y}$および前記ノードパラメータ$\gamma_{x,y}$に基づいて、鍵を算出する鍵算出ステップと、

を備える、鍵生成方法。

【請求項１６】

ｎ個の受信装置のなかから排除する受信装置を特定し、排除されていない受信装置の集合Ｓを決定する、排除受信装置特定ステップを備える、暗号化方法。

【請求項１７】

ｎ個の受信装置がリーフに割り当てられ、高さが（$\log_Y n$）で表されるＹ分木構造を階層的に構成し、前記リーフとルートとの間に存在する中間ノードの下位に存在する複数の前記リーフからなるサブグループを構成し、前記リーフおよび前記中間ノードそれぞ

れに対して、リーフキーg_yを割り当て、前記中間ノードおよび前記ルートに、相異なるパラメータ$\nu_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とノードパラメータ$\gamma_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とをそれぞれ割り当て、前記ルートから前記リーフに至るパスを特定し、当該パス上に存在する前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yと、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\nu_{x,y}$および前記ノードパラメータ$\gamma_{x,y}$に基づいて算出された鍵を受信するステップを備える、鍵処理方法。

【請求項１８】

コンピュータに、

ｎ個の受信装置がリーフに割り当てられ、高さが（$\log_Y n$）で表されるＹ分木構造を階層的に構成し、前記リーフとルートとの間に存在する中間ノードの下位に存在する複数の前記リーフからなるサブグループを構成する、木構造構成機能と、

前記リーフおよび前記中間ノードそれぞれに対して、リーフキーg_yを割り当てるリーフキー割当機能と、

前記中間ノードおよび前記ルートに、相異なるパラメータ$\nu_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とノードパラメータ$\gamma_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とをそれぞれ割り当てるパラメータ割当機能と、

前記ルートから前記リーフに至るパスを特定し、当該パス上に存在する前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yと、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\nu_{x,y}$および前記ノードパラメータ$\gamma_{x,y}$に基づいて、鍵を算出する鍵算出機能と、

を実現させるためのプログラム。

【請求項１９】

コンピュータに、ｎ個の受信装置のなかから排除する受信装置を特定し、排除されていない受信装置の集合Ｓを決定する、排除受信装置特定機能を実現させるためのプログラム。

【請求項２０】

コンピュータに、ｎ個の受信装置がリーフに割り当てられ、高さが（$\log_Y n$）で表されるＹ分木構造を階層的に構成し、前記リーフとルートとの間に存在する中間ノードの下位に存在する複数の前記リーフからなるサブグループを構成し、前記リーフおよび前記中間ノードそれぞれに対して、リーフキーg_yを割り当て、前記中間ノードおよび前記ルートに、相異なるパラメータ$\nu_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とノードパラメータ$\gamma_{x,y}$（ｘ：階層、ｙ：１，２，・・・，Y^x）とをそれぞれ割り当て、前記ルートから前記リーフに至るパスを特定し、当該パス上に存在する前記中間ノードまたは前記リーフに割り当てられた前記リーフキーg_yと、当該中間ノードまたは当該リーフの親ノードに割り当てられた前記パラメータ$\nu_{x,y}$および前記ノードパラメータ$\gamma_{x,y}$に基づいて算出された暗号鍵を受信する受信機能を実現させるためのプログラム。