【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28年4月21日(2016.4.21)

【公表番号】特表2015-520967(P2015-520967A)
【公表日】平成27年7月23日(2015.7.23)
【年通号数】公開・登録公報2015-046
【出願番号】特願2015-509562(P2015-509562)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｗ　4/06　(2009.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｂ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｗ　12/04
Ｈ０４Ｗ　4/06　１５０

【手続補正書】
【提出日】平成28年3月2日(2016.3.2)
【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】
ブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）において、マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）トラフィック鍵（ＭＴＫ）を生成する方法であって、
集中化した鍵管理サービスで生成されるＭＢＭＳサービス鍵（ＭＳＫ）を受信するステップと、
少なくとも受信した前記ＭＳＫの関数として、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化する際に使用される前記ＭＴＫを生成するステップと
を含むことを特徴とする方法。
【請求項２】
受信する前記ステップは、ネットワークインターフェースを介して前記集中化した鍵管理サービスから前記ＭＳＫを受信するステップを含むことを特徴とする請求項１に記載の方法。
【請求項３】
受信する前記ステップは、前記集中化した鍵管理サービスの代わりに前記ＭＳＫを送信するスタンドアロンサーバからの該ＭＳＫをネットワークインターフェースを介して受信するステップを含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記ＭＴＫは、受信した前記ＭＳＫ及びＭＴＫシード値の関数として生成されることを特徴とする請求項１に記載の方法。
【請求項５】
前記関数は、標準化鍵生成関数であることを特徴とする請求項４に記載の方法。
【請求項６】
前記標準化鍵生成関数は、第三世代パートナーシップ・プロジェクトの技術仕様書３３

．２２０で定義されている鍵生成関数であることを特徴とする請求項５に記載の方法。
【請求項７】
前記ＭＴＫは、受信した前記ＭＳＫ、ＭＲＫ、及びＣＫ｜｜ＩＫに関連付けられた、サービスＩＤ、鍵ドメインＩＤ、及びＭＳＫ－ＩＤを含むリストから選択された少なくとも１つのパラメータの関数としても生成されることを特徴とする請求項４に記載の方法。
【請求項８】
前記少なくとも１つのパラメータは、前記ＫＤＦへ入力される前に変換されることを特徴とする請求項７に記載の方法。
【請求項９】
前記ＭＴＫ－ＩＤは、シーケンス番号であることを特徴とする請求項７に記載の方法。
【請求項１０】
前記ＭＴＫシード値は、ＭＴＫ生成鍵、及びＭＴＫ－ＩＤの関数として生成されることを特徴とする請求項４に記載の方法。
【請求項１１】
前記ＭＴＫ生成鍵は、前記ＢＭＳＣには知られているものの、前記ＵＥへは知られていないことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記ＭＴＫ生成鍵は、前記集中化した鍵管理サービスによって提供されることを特徴とする請求項１０に記載の方法。
【請求項１３】
前記ＭＴＫ生成鍵は、静的な値として、前記集中化した鍵管理サービスによって提供されることを特徴とする請求項１２に記載の方法。
【請求項１４】
前記ＭＴＫ生成鍵は、周期的に、前記集中化した鍵管理サービスによって提供されることを特徴とする請求項１２に記載の方法。
【請求項１５】
コンテンツを確保するための鍵を配信する、集中化された鍵管理サーバで実行される方法であって、
ＭＢＭＳサービス鍵（ＭＳＫ）を生成するステップと、
マルチメディア・ブロードキャスト・マルチキャスト・トラフィック鍵（ＭＴＫ）を送信することなく、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化するＭＴＫを生成する際に使用される前記生成されたＭＳＫをブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）へ送信するステップと、
少なくとも前記送信したＭＳＫの関数として、前記ＢＭＳＣで生成される前記ＭＴＫを用いて、前記ＢＭＳＣによって送信され、かつ暗号化された前記コンテンツのストリームを復号化するために、前記ＵＥ用の復号化鍵を該ＵＥへ送信するステップと
を含むことを特徴とする方法。
【請求項１６】
前記復号化鍵は、前記ＢＭＳＣへ送信されない前記ＭＴＫであることを特徴とする請求項１５に記載の方法。
【請求項１７】
前記生成したＭＳＫを送信するステップは、前記ＢＭＳＣへ配信するためにスタンドアロンサーバへ前記生成したＭＳＫを送信するステップを含むことを特徴とする請求項１５に記載の方法。
【請求項１８】
前記ＢＭＳＣへ鍵生成関数を送信するステップをさらに含み、
前記鍵生成関数は、前記ＭＳＫに従ってＭＴＫを生成する際に前記ＢＭＳＣによって使用され、
前記生成されたＭＴＫ及び前記ＭＳＫは、前記コンテンツのストリームを暗号化するために使用されることを特徴とする請求項１５に記載の方法。

【請求項１９】
受信した前記ＭＳＫ、ＭＲＫ、及びＣＫ｜｜ＩＫに関連付けられたサービスＩＤ、鍵ドメインＩＤ、及びＭＳＫ－ＩＤの少なくとも１つを前記ＢＭＳＣへ送信するステップをさらに含むことを特徴とする請求項１５に記載の方法。
【請求項２０】
ブロードキャスト・マルチキャスト・サービス・センター・ノードであって、
ユーザ機器ノード及び集中化した鍵管理サーバと通信を行うネットワーク・インターフェースと、
命令を格納するメモリと、
前記格納された命令を実行するプロセッサであって、該格納された命令を実行すると、前記ブロードキャスト・マルチキャスト・サービス・センター・ノードが、
少なくとも前記集中化した鍵管理サーバで生成されるＭＢＭＳサービス鍵（ＭＳＫ）の関数として、前記ユーザ機器ノードへ送信されるコンテンツを暗号化に使用するための、マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）トラフィック鍵（ＭＴＫ）を生成する、
前記プロセッサと
を備えることを特徴とするブロードキャスト・マルチキャスト・サービス・センター・ノード。
【請求項２１】
集中化した鍵管理サーバであって、
ユーザ機器ノードと、ブロードキャスト・マルチキャスト・サービス・センター・ノードと通信するためのネットワークインターフェースと、
命令を格納するメモリと、
前記格納された命令を実行するプロセッサであって、該格納された命令を実行すると、前記集中化した鍵管理サーバが、
マルチメディア・ブロードキャスト・マルチキャスト・サービス（ＭＢＭＳ）サービス鍵（ＭＳＫ）を生成し、
対応するＭＢＭＳトラフィック鍵（ＭＴＫ）を送信することなく、ユーザ機器ノード（ＵＥ）へ送信されるコンテンツを暗号化するＭＴＫを生成する際に使用される前記生成されたＭＳＫを、ブロードキャスト・マルチキャスト・サービス・センター（ＢＭＳＣ）へ送信し、
前記ＵＥへ対して、少なくとも前記送信したＭＳＫの関数として、前記ＢＭＳＣで生成される前記ＭＴＫを用いて、前記ＢＭＳＣによって送信され、かつ暗号化された前記コンテンツのストリームを復号化するために、前記ＵＥ用の復号化鍵を送信する、
前記プロセッサと
を備えることを特徴とする集中化した鍵管理サーバ。