【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27年1月29日(2015.1.29)

【公表番号】特表2014-508436(P2014-508436A)
【公表日】平成26年4月3日(2014.4.3)
【年通号数】公開・登録公報2014-017
【出願番号】特願2013-548363(P2013-548363)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/62　(2013.01)
Ｈ０４Ｗ　12/08　(2009.01)
Ｈ０４Ｍ　11/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｇ０６Ｆ　21/24　１６６Ａ
Ｈ０４Ｗ　12/08
Ｈ０４Ｍ　11/00　３０２

【手続補正書】
【提出日】平成26年12月8日(2014.12.8)
【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】
無線通信システムにおける端末により短文データを暗号化する方法であって、
アイドルモードで短文データバーストを生成するステップと、
認証キー(ＡＫ)から導出されるＣＭＡＣ(Cipher-based Message Authentication Code)-トラフィック暗号化キー(ＴＥＫ)プレキーに基づいてＴＥＫを生成するステップと、
前記端末で、レンジング要求(ＲＮＧ-ＲＥＱ)メッセージと一緒に伝送されるアップリンクＣＭＡＣパケット番号(ＣＭＡＣ-ＰＮ_Ｕ)と同一の値であるパケット番号(ＰＮ)に基づいてノンスを構成するステップと、
前記ＴＥＫ及び前記ノンスに基づいて前記短文データバーストを暗号化するステップと、
メディアアクセス制御(ＭＡＣ)ヘッダーと、前記暗号化された短文データバーストと、ＣＭＡＣダイジェストを含むＭＡＣ　ＰＤＵ(Protocol Data Unit)を生成するステップと、
前記ＭＡＣ　ＰＤＵを基地局に伝送するステップと、を有することを特徴とする方法。
【請求項２】
前記ＲＮＧ-ＲＥＱメッセージは、前記暗号化された短文データを含み、前記ＣＭＡＣダイジェストは、前記ＣＭＡＣ-ＰＮ_Ｕ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】
前記ＲＮＧ-ＲＥＱメッセージは、
前記ＲＮＧ-ＲＥＱメッセージが前記アイドルモードで位置更新のために伝送されることを指示するレンジング目的指示フィールドと、
前記ＲＮＧ-ＲＥＱメッセージがＣＭＡＣにより保護されるか否かを示すＣＭＡＣイン

ジケータと、
前記暗号化された短文データバーストと、を含むことを特徴とする請求項２に記載の方法。
【請求項４】
前記ＲＮＧ-ＲＥＱメッセージは、
前記ＲＮＧ-ＲＥＱメッセージに含まれる前記短文データバーストが暗号化されるか否かを示す暗号化インジケータをさらに含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記ノンスは、
前記短文データバーストの長さ、端末識別子(ＳＴＩＤ)、フロー識別子(ＦＩＤ)、所定個数の０、及び前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項１に記載の方法。
【請求項６】
ネットワーク初期進入手順で獲得したマスタセッションキー(ＭＳＫ)を切り詰めて双方向マスタキー(ＰＭＫ)を生成するステップと、
前記ＰＭＫ、前記端末のアドレス、及び前記基地局の識別子(ＩＤ)を用いて前記端末と前記基地局との間のＳＡに対するＡＫを生成するステップと、
前記ＡＫを用いて前記ＣＭＡＣ-ＴＥＫプレキーを生成するステップと、を有し、
前記ＴＥＫは、前記ＣＭＡＣ-ＴＥＫプレキーと、前記端末と前記基地局との間のＳＡに対するＳＡ識別子(ＳＡＩＤ)と、前記ＴＥＫに対するＴＥＫカウンタ値を用いて生成され、
前記ＳＡＩＤと前記ＴＥＫカウンタ値は予め設定されることを特徴とする請求項１に記載の方法。
【請求項７】
前記短文データバーストは、短文メッセージサービス（ＳＭＳ)ペイロードであることを特徴とする請求項１に記載の方法。
【請求項８】
無線通信システムにおける基地局(ＢＳ)により短文データを復号化する方法であって、
端末からメディアアクセス制御(ＭＡＣ)ヘッダーと、暗号化された短文データバーストと、ＣＭＡＣ(Cipher-based Message Authentication Code)ダイジェストを含むＭＡＣプロトコルデータユニット(ＰＤＵ)を受信するステップと、
認証キー(ＡＫ)から派生したＣＭＡＣ-トラフィック暗号化キー(ＴＥＫ)プレキーに基づいてＴＥＫを生成するステップと、
前記ＣＭＡＣダイジェストに含まれたアップリンクＣＭＡＣパケット番号(ＣＭＡＣ-ＰＮ_Ｕ)と同一の値であるパケット番号(ＰＮ)に基づいてノンスを構成するステップと、
前記ＴＥＫ及び前記ノンスに基づいて前記暗号化された短文データバーストを復号化するステップと、を有することを特徴とする方法。
【請求項９】
前記ＭＡＣ ＰＤＵは、前記暗号化された短文データバーストを含み、前記ＣＭＡＣダイジェストは、前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項８に記載の方法。
【請求項１０】
前記ＲＮＧ-ＲＥＱメッセージは、
前記ＲＮＧ-ＲＥＱメッセージがアイドルモードで位置更新のために伝送されることを指示するレンジング目的指示フィールドと、
前記ＲＮＧ-ＲＥＱメッセージがＣＭＡＣにより保護されるか否かを示すＣＭＡＣインジケータと、
前記暗号化された短文データバーストと、を含むことを特徴とする請求項９に記載の方法。
【請求項１１】
前記ＲＮＧ-ＲＥＱメッセージは、
前記ＲＮＧ-ＲＥＱメッセージに含まれる前記短文データバーストが暗号化されるか否

かを示す暗号化インジケータを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記ノンスは、
前記短文データバーストの長さ、端末識別子(ＳＴＩＤ)、フロー識別子(ＦＩＤ)、所定個数の０、及び前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項８に記載の方法。
【請求項１３】
ＳＡに関連して獲得したマスタセッションキー(ＭＳＫ)を切り詰めて双方向マスタキー(ＰＭＫ)を生成するステップと、
前記ＰＭＫ、前記端末のアドレス、及び前記基地局の識別子(ＩＤ)を用いて前記端末と前記基地局との間のＳＡに対する前記ＡＫを生成するステップと、
前記ＡＫを用いて前記ＣＭＡＣ-ＴＥＫプレキーを生成するステップと、をさらに有し、
前記ＴＥＫは、前記ＣＭＡＣ-ＴＥＫプレキー、前記端末と前記基地局との間のＳＡに対するＳＡ識別子(ＳＡＩＤ)、及び前記ＴＥＫに対するＴＥＫカウンタ値を用いて生成され、
前記ＳＡＩＤと前記ＴＥＫカウンタ値は予め設定されることを特徴とする請求項８に記載の方法。
【請求項１４】
前記短文データバーストは、短文メッセージサービス（ＳＭＳ)ペイロードであることを特徴とする請求項８に記載の方法。
【請求項１５】
無線通信システムにおける短文データを暗号化する端末装置であって、
アイドルモードで短文データバーストを生成するように構成される生成部と、
認証キー(ＡＫ）から導出するＣＭＡＣ(Cipher-based Message Authentication Code)-トラフィック暗号化キー(ＴＥＫ)プレキーに基づいてＴＥＫを生成し、レンジング要求(ＲＮＧ-ＲＥＱ)メッセージと一緒に伝送されるアップリンクＣＭＡＣパケット番号(ＣＭＡＣ-ＰＮ_Ｕ)と同一の値であるパケット番号(ＰＮ)に基づいてノンスを構成し、前記ＴＥＫ及び前記ノンスに基づいて前記短文データバーストを暗号化する暗号化部と、
メディアアクセス制御(ＭＡＣ)ヘッダーと、前記暗号化された短文データバーストと、ＣＭＡＣダイジェストを含むＭＡＣプロトコルデータユニット(ＰＤＵ)を生成し、前記ＭＡＣ ＰＤＵを基地局(ＢＳ)に伝送する伝送部と、を含むことを特徴とする端末装置。
【請求項１６】
前記ＲＮＧ-ＲＥＱメッセージは、前記暗号化された短文データを含み、前記ＣＭＡＣダイジェストは、前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項１５に記載の端末装置。
【請求項１７】
前記ＲＮＧ-ＲＥＱメッセージは、
前記ＲＮＧ-ＲＥＱメッセージが前記アイドルモードで位置更新のために伝送されることを指示するレンジング目的指示フィールドと、
前記ＲＮＧ-ＲＥＱメッセージがＣＭＡＣにより保護されるか否かを示すＣＭＡＣインジケータと、
前記暗号化された短文データバーストと、を含むことを特徴とする請求項１６に記載の端末装置。
【請求項１８】
前記ＲＮＧ-ＲＥＱメッセージは、
前記ＲＮＧ-ＲＥＱメッセージに含まれる前記短文データバーストが暗号化されるか否かを示す暗号化インジケータをさらに含むことを特徴とする請求項１６に記載の端末装置。
【請求項１９】
前記ノンスは、

前記短文データバーストの長さ、端末識別子(ＳＴＩＤ)、フロー識別子(ＦＩＤ)、所定個数の０、及び前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項１５に記載の端末装置。

【請求項２０】

ネットワーク初期進入手順で獲得したマスタセッションキー(ＭＳＫ)を切り詰めて双方向マスタキー(ＰＭＫ)を生成し、前記ＰＭＫ、端末のアドレス、及び前記基地局(ＢＳ)の識別子(ＩＤ)を用いて前記端末と前記基地局との間のＳＡに対する認証キー(ＡＫ)を生成し、前記ＡＫを用いて前記ＣＭＡＣ-ＴＥＫプレキーを生成する制御部をさらに含み、

前記ＴＥＫは、前記ＣＭＡＣ-ＴＥＫプレキー、前記端末と前記基地局との間のＳＡに対するＳＡ識別子(ＳＡＩＤ)と、前記ＴＥＫに対するＴＥＫカウンタ値を用いて生成され、

前記ＳＡＩＤと前記ＴＥＫカウンタ値は予め設定されることを特徴とする請求項１５に記載の端末装置。

【請求項２１】

前記短文データバーストは、短文メッセージサービス（ＳＭＳ)ペイロードであることを特徴とする請求項１５に記載の端末装置。

【請求項２２】

無線通信システムにおける短文データを復号化する基地局(ＢＳ)装置であって、

端末からメディアアクセス制御(ＭＡＣ)ヘッダーと、暗号化された短文データバーストと、ＣＭＡＣ(Cipher-based Message Authentication Code)ダイジェストを含むＭＡＣプロトコルデータユニット(ＰＤＵ)を受信する受信部と、

認証キー(ＡＫ)から派生した、ＣＭＡＣ-トラフィック暗号化キー(ＴＥＫ)プレキーに基づいてＴＥＫを生成し、前記ＣＭＡＣダイジェストに含まれたアップリンクＣＭＡＣパケット番号(ＣＭＡＣ-ＰＮ_Ｕ)と同一の値であるパケット番号(ＰＮ)に基づいてノンスを構成し、前記ＴＥＫ及び前記ノンスに基づいて前記暗号化された短文データバーストを復号化する復号化部と、を含む

ことを特徴とする基地局装置。

【請求項２３】

前記ＭＡＣ ＰＤＵは、前記暗号化された短文データバーストを含み、前記ＣＭＡＣダイジェストは、前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項２２に記載の基地局装置。

【請求項２４】

前記ＲＮＧ-ＲＥＱメッセージは、

前記ＲＮＧ-ＲＥＱメッセージがアイドルモードで位置更新のために伝送されることを指示するレンジング目的指示フィールドと、

前記ＲＮＧ-ＲＥＱメッセージがＣＭＡＣにより保護されるか否かを示すＣＭＡＣインジケータと、

前記暗号化された短文データバーストと、を含むことを特徴とする請求項２３に記載の基地局装置。

【請求項２５】

前記ＲＮＧ-ＲＥＱメッセージは、

前記ＲＮＧ-ＲＥＱメッセージに含まれる前記短文データバーストが暗号化されるか否かを示す暗号化インジケータを含むことを特徴とする請求項２４に記載の基地局装置。

【請求項２６】

前記ノンスは、

前記短文データバーストの長さ、端末識別子(ＳＴＩＤ)、フロー識別子(ＦＩＤ)、所定の個数０、及び前記ＣＭＡＣ-ＰＮ_Ｕを含むことを特徴とする請求項２２に記載の基地局装置。

【請求項２７】

ＳＡに関連して獲得したマスタセッションキー(ＭＳＫ)を切り詰めて双方向マスタキー

(ＰＭＫ)を生成し、前記ＰＭＫ、前記端末のアドレス、前記基地局(ＢＳ)の識別子を用いて前記端末と前記ＢＳとの間のＳＡに対する前記ＡＫを生成し、前記ＡＫを用いて前記ＣＭＡＣ-ＴＥＫプレキーを生成する制御部をさらに含み、

前記ＴＥＫは、前記ＣＭＡＣ-ＴＥＫプレキー、前記端末と前記ＢＳとの間のＳＡに対するＳＡ識別子(ＳＡＩＤ)、及び前記ＴＥＫに対するＴＥＫカウンタ値を用いて生成され、

前記ＳＡＩＤと前記ＴＥＫカウンタ値は予め設定されることを特徴とする請求項２２に記載の基地局装置。

【請求項２８】

前記短文データバーストは、短文メッセージサービス（ＳＭＳ)ペイロードであることを特徴とする請求項２２に記載の基地局装置。