【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26年12月18日(2014.12.18)

【公開番号】特開2014-180062(P2014-180062A)
【公開日】平成26年9月25日(2014.9.25)
【年通号数】公開・登録公報2014-052
【出願番号】特願2014-137760(P2014-137760)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成26年10月31日(2014.10.31)
【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】
汎用集積回路カード（ＵＩＣＣ）と端末との間の通信をセキュアにするための方法であって、前記方法は、
セキュア共有セッション鍵を生成するステップと、
前記ＵＩＣＣと前記端末との間の通信を、前記セキュア共有セッション鍵を用いて暗号化するステップと
を備えることを特徴とする方法。
【請求項２】
前記セキュア共有セッション鍵を生成するステップは、共有秘密から前記セキュア共有セッション鍵を導き出す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】
前記共有秘密から前記セキュア共有セッション鍵を導き出すステップは、秘密から共有秘密を生成するステップ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】
前記セキュア共有セッション鍵を導き出すステップは、前記共有秘密を使用して、擬似乱数関数（ＰＲＦ）を実行するステップを含むことを特徴とする請求項２に記載の方法。
【請求項５】
前記通信を暗号化するステップは、セキュアチャネルを確立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６】
前記セキュアチャネルを使用して、アプリケーションレベルのＵＩＣＣベースの拡張を伴う汎用ブートストラッピングアーキテクチャ（ＧＢＡ）（ＧＢＡ　Ｕ）手続き、またはＡＫＡ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ａｇｒｅｅｍｅｎｔ）手続きの少なくとも１つを実行するステップをさらに備え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ＵＩＣＣと前記端末との間のインタフェース上でトンネルを作成するステップをさらに備えることを特徴とする請求項１に記載の方法。

【請求項８】
前記セキュア共有セッション鍵を生成するステップは、
セキュア共有セッション鍵が、前記ＵＩＣＣと前記端末との間に存在するかどうかを判定するステップと、
セキュア共有セッション鍵が存在しないという条件で、新たなセキュア共有セッション鍵を生成するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項９】
前記セキュア共有セッション鍵を生成するステップは、
作り出される鍵ネゴシエーションパラメータを作り出すステップと、
前記作り出された鍵ネゴシエーションパラメータを前記ＵＩＣＣに報告するステップと、
受信される鍵ネゴシエーションパラメータを受信するステップと、
前記作り出された鍵ネゴシエーションパラメータ、および前記受信された鍵ネゴシエーションパラメータを使用して、前記セキュア共有セッション鍵を作成するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項１０】
前記作成するステップは、
前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるかどうかを判定するステップと、
前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるという条件で、セキュア共有セッション鍵を導き出すステップと
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】
前記作り出すステップは、
ランダムチャレンジ（ＲＡＮＤ）およびシーケンス番号（ＳＱＮ）を選択するステップと、
匿名鍵（ＡＫ）、メッセージ認証コード（ＭＡＣ）、予想応答（ＸＲＥＳ）、および予想シーケンス（ＸＳＱＮ）を計算するステップと、
前記ＲＡＮＤ、前記ＭＡＣ、および前記ＸＳＱＮを組み合わせて、前記作り出される鍵ネゴシエーションパラメータを作り出すステップと
を含むことを特徴とする請求項９に記載の方法。
【請求項１２】
前記計算するステップは、
共有秘密および前記ＲＡＮＤを使用して前記ＡＫを計算するステップと、
前記共有秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＭＡＣを計算するステップと、
前記共有秘密および前記ＲＡＮＤを使用して前記ＸＲＥＳを計算するステップと、
前記ＳＱＮおよび前記ＡＫを使用して前記ＸＳＱＮを計算するステップと
を含むことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記作り出すステップは、
ノンスを選択するステップと、
認証値（Ｔａｇ）を計算するステップと、
前記ノンスと前記Ｔａｇを組み合わせて、前記作り出される鍵ネゴシエーションパラメータを作り出すステップと
を含むことを特徴とする請求項９に記載の方法。
【請求項１４】
前記作り出すステップは、

セッション鍵を選択するステップと、
暗号化されたセッション鍵を計算するステップと、
前記暗号化されたセッション鍵を使用して、前記鍵ネゴシエーションパラメータを作り出すステップと
を含むことを特徴とする請求項９に記載の方法。
【請求項１５】
前記セキュア共有セッション鍵を生成するステップは、
受信される鍵ネゴシエーションパラメータを受信するステップと、
作り出される鍵ネゴシエーションパラメータを作り出すステップと、
前記作り出された鍵ネゴシエーションパラメータを前記端末に報告するステップと、
前記受信された鍵ネゴシエーションパラメータ、および前記作り出された鍵ネゴシエーションパラメータを使用して、前記セキュア共有セッション鍵を作成するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項１６】
前記作成するステップは、
前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるかどうかを判定するステップと、
前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるという条件で、セキュア共有セッション鍵を導き出すステップと
を含むことを特徴とする請求項１５に記載の方法。
【請求項１７】
前記作り出すステップは、
前記受信された鍵ネゴシエーションパラメータから、ランダムチャレンジ（ＲＡＮＤ）、メッセージ認証コード（ＭＡＣ）、および予想シーケンス（ＸＳＱＮ）を抽出するステップと、
匿名鍵（ＡＫ）、予想メッセージ認証コード（ＸＭＡＣ）、およびＳＱＮ（シーケンス番号）を計算するステップと、
前記ＸＭＡＣが前記ＭＡＣと同一であるかどうかを判定するステップと、
前記ＸＭＡＣが前記ＭＡＣと同一であるという条件で、共有秘密および前記ＲＡＮＤを使用して応答（ＲＥＳ）を計算するステップと
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】
前記計算するステップは、
前記共有秘密および前記ＲＡＮＤを使用して前記ＡＫを計算するステップと、
前記ＸＳＱＮおよび前記ＡＫを使用して前記ＳＱＮを計算するステップと、
前記共有秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＸＭＡＣを計算するステップと
を含むことを特徴とする請求項１７に記載の方法。
【請求項１９】
前記作り出すステップは、
前記受信された鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出するステップと、
前記Ｔａｇを検証するステップと、
前記Ｔａｇが有効であるという条件で、セッション鍵を導き出し、および予想認証値（ＸＴａｇ）を計算するステップと、
前記ＸＴａｇを使用して、前記作り出される鍵ネゴシエーションパラメータを作り出すステップと
を含むことを特徴とする請求項１５に記載の方法。
【請求項２０】

前記作り出すステップは、前記受信された鍵ネゴシエーションパラメータから前記暗号化されたセッション鍵を抽出するステップを含み、および前記セッション鍵を導き出すことは、前記暗号化されたセッション鍵を復号することを含むことを特徴とする請求項１９に記載の方法。
【請求項２１】
前記セキュア共有セッション鍵を生成するステップは、
事前鍵ネゴシエーションパラメータを生成するステップと、
前記事前鍵ネゴシエーションパラメータを前記端末に報告するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項２２】
前記セキュア共有セッション鍵を生成するステップは、前記ＵＩＣＣから事前鍵ネゴシエーションパラメータ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２３】
前記生成するステップは、ディフィーヘルマン鍵交換プロトコルを実行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２４】
セキュア共有セッション鍵を生成し、
前記セキュア共有セッション鍵を用いて通信を暗号化し、
前記暗号化された通信を送信し、
前記セキュア共有セッション鍵を使用して、受信され暗号化された通信を復号するように構成された汎用集積回路カード（ＵＩＣＣ）と、
前記セキュア共有セッション鍵を生成し、
前記セキュア共有セッション鍵を用いて通信を暗号化し、
前記暗号化された通信を送信し、
前記セキュア共有セッション鍵を使用して、受信され暗号化された通信を復号するように構成された端末と
を備えたことを特徴とするＷＴＲＵ（無線送信／受信ユニット）。
【請求項２５】
前記ＵＩＣＣは、共有秘密から前記セキュア共有セッション鍵を導き出すことによって、前記セキュア共有セッション鍵を生成するように構成され、および前記端末は、前記共有秘密から前記セキュア共有セッション鍵を導き出すことによって、前記セキュア共有セッション鍵を生成するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項２６】
前記ＵＩＣＣは、第１の秘密から前記共有秘密を生成することによって、前記共有秘密から前記セキュア共有セッション鍵を導き出すように構成され、および前記端末は、第２の秘密から前記共有秘密を生成することによって、前記共有秘密から前記セキュア共有セッション鍵を導き出すように構成されることを特徴とする請求項２５に記載のＷＴＲＵ。
【請求項２７】
前記ＵＩＣＣは、前記共有秘密を使用して擬似乱数関数（ＰＲＦ）を実行することによって、前記セキュア共有セッション鍵を導き出すように構成され、および前記端末は、前記共有秘密を使用して前記擬似乱数関数（ＰＲＦ）を実行することによって、前記セキュア共有セッション鍵を導き出すように構成されることを特徴とする請求項２５に記載のＷＴＲＵ。
【請求項２８】
前記ＵＩＣＣは、前記端末とセキュアチャネルを確立するように構成され、および前記端末は、前記ＵＩＣＣとセキュアチャネルを確立するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項２９】
前記端末は、前記セキュアチャネルを使用して、アプリケーションレベルのＵＩＣＣベ

ースの拡張を伴う汎用ブートストラッピングアーキテクチャ（ＧＢＡ）（ＧＢＡ　Ｕ）手続き、またはＡＫＡ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ａｇｒｅｅｍｅｎｔ）手続きの少なくとも１つを実行するように構成されることを特徴とする請求項２８に記載のＷＴＲＵ。

【請求項３０】

前記端末は、

作り出される鍵ネゴシエーションパラメータを作り出し、

前記作り出された鍵ネゴシエーションパラメータを前記ＵＩＣＣに報告し、

前記ＵＩＣＣから、受信される鍵ネゴシエーションパラメータを受信し、

前記作り出された鍵ネゴシエーションパラメータ、および前記受信された鍵ネゴシエーションパラメータを使用して、前記セキュア共有セッション鍵を生成するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。

【請求項３１】

前記端末は、

前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるかどうかを判定し、

前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるという条件で、前記セキュア共有セッション鍵を生成するように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。

【請求項３２】

前記端末は、

ランダムチャレンジ（ＲＡＮＤ）およびシーケンス番号（ＳＱＮ）を選択し、

匿名鍵（ＡＫ）、メッセージ認証コード（ＭＡＣ）、予想応答（ＸＲＥＳ）、および予想シーケンス（ＸＳＱＮ）を計算し、

前記ＲＡＮＤ、前記ＭＡＣ、および前記ＸＳＱＮを使用して、前記作り出される鍵ネゴシエーションパラメータを作り出すように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。

【請求項３３】

前記端末は、

共有秘密と前記ＲＡＮＤを使用して前記ＡＫを計算し、

前記共有秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＭＡＣを計算し、

前記共有秘密および前記ＲＡＮＤを使用して前記ＸＲＥＳを計算し、

前記ＳＱＮおよび前記ＡＫを使用して前記ＸＳＱＮを計算するように構成されることを特徴とする請求項３２に記載のＷＴＲＵ。

【請求項３４】

前記端末は、

ノンスを選択し、

認証値（Ｔａｇ）を計算し、

前記ノンスおよび前記Ｔａｇを使用して、前記作り出される鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。

【請求項３５】

前記端末は、

セッション鍵を選択し、

暗号化されたセッション鍵を計算し、

前記暗号化されたセッション鍵を使用して、前記作り出される鍵ネゴシエーションパラメータを作り出すように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。

【請求項３６】

前記ＵＩＣＣは、

前記端末から、受信される鍵ネゴシエーションパラメータを受信し、

作り出される鍵ネゴシエーションパラメータを作り出し、

前記作り出された鍵ネゴシエーションパラメータを前記端末に報告し、
前記受信された鍵ネゴシエーションパラメータ、および前記作り出された鍵ネゴシエーションパラメータを使用して、前記セキュア共有セッション鍵を生成するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項３７】
前記ＵＩＣＣは、
前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるかどうかを判定し、
前記作り出された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるという条件で、前記セキュア共有セッション鍵を生成するように構成されることを特徴とする請求項３６に記載のＷＴＲＵ。
【請求項３８】
前記ＵＩＣＣは、
前記受信された鍵ネゴシエーションパラメータから、ランダムチャレンジ（ＲＡＮＤ）、メッセージ認証コード（ＭＡＣ）、および予想シーケンス（ＸＳＱＮ）を抽出し、
匿名鍵（ＡＫ）、予想メッセージ認証コード（ＸＭＡＣ）、およびシーケンス番号（ＳＱＮ）を計算し、
前記ＸＭＡＣが前記ＭＡＣと同一であるかどうかを判定し、
前記ＸＭＡＣが前記ＭＡＣと同一であるという条件で、共有秘密および前記ＲＡＮＤを使用して応答（ＲＥＳ）を計算し、
前記ＲＥＳを使用して、前記作り出される鍵ネゴシエーションパラメータを作り出すように構成されることを特徴とする請求項３６に記載のＷＴＲＵ。
【請求項３９】
前記ＵＩＣＣは、
前記共有秘密および前記ＲＡＮＤを使用して前記ＡＫを計算し、
前記ＸＳＱＮおよび前記ＡＫを使用して前記ＳＱＮを計算し、
前記共有秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＸＭＡＣを計算するように構成されることを特徴とする請求項３８に記載のＷＴＲＵ。
【請求項４０】
前記ＵＩＣＣは、
前記受信された鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出し、
前記Ｔａｇを検証し、
予想認証値（ＸＴａｇ）を計算し、
前記ＸＴａｇを使用して、前記作り出される鍵ネゴシエーションパラメータを作り出すように構成されることを特徴とする請求項３６に記載のＷＴＲＵ。
【請求項４１】
前記ＵＩＣＣは、
前記受信された鍵ネゴシエーションパラメータから暗号化されたセッション鍵を抽出し、
前記暗号化されたセッション鍵を復号し、
前記復号されたセッション鍵を使用して、前記セキュア共有セッション鍵を生成するように構成されることを特徴とする請求項４０に記載のＷＴＲＵ。
【請求項４２】
前記ＵＩＣＣは、
事前鍵ネゴシエーションパラメータを生成し、
前記事前鍵ネゴシエーションパラメータを前記端末に報告するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項４３】
前記端末は、事前鍵ネゴシエーションパラメータを前記ＵＩＣＣから受信するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。

【請求項４４】
前記ＵＩＣＣは、ディフィーヘルマン鍵交換プロトコルを実行するように構成され、および前記端末は、ディフィーヘルマン鍵交換プロトコルを実行するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。