(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2024-81663
(P2024-81663A)
(43)公開日　令和6年6月18日(2024.6.18)

(51)国際特許分類　FI
H04L 9/32 (2006.01)　H04L 9/32 200A
H04L 9/32 200F

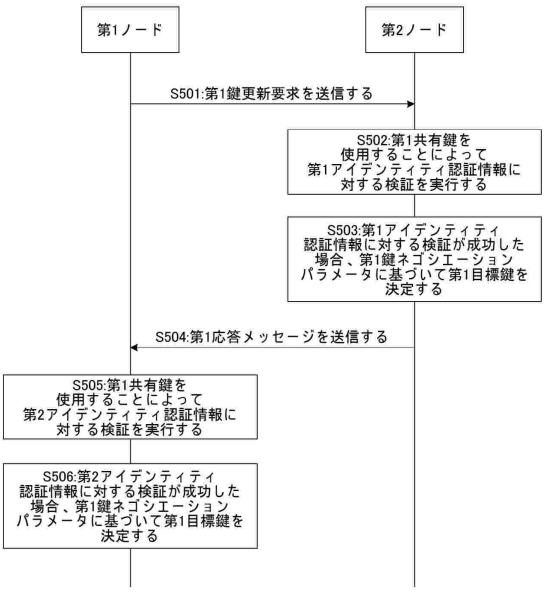
審査請求　有　請求項の数　24　OL　外国語出願　（全81頁）

(21)出願番号　特願2024-34390(P2024-34390)
(22)出願日　令和6年3月6日(2024.3.6)
(62)分割の表示　特願2022-550128(P2022-550128)の分割
原出願日　令和2年2月29日(2020.2.29)

(71)出願人　504161984
ホアウェイ・テクノロジーズ・カンパニー・リミテッド
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング
(74)代理人　110000877
弁理士法人ＲＹＵＫＡ国際特許事務所
(72)発明者　ワン、ヨン
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション
最終頁に続く

(54)【発明の名称】　鍵更新方法および関連装置

(57)【要約】　（修正有）
【課題】鍵更新プロセスにおけるデータセキュリティを改善するための鍵更新方法及び装置を提供する。
【解決手段】鍵更新方法において、第１ノードは、第２ノードへ第１鍵更新要求を送信するＳ５０１。第１鍵更新要求は、第１鍵ネゴシエーションパラメータ及び第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される。次いで、第２ノードは、第１ノードへ第２アイデンティティ認証情報を含む第１応答メッセージを送信するＳ５０４。その後、第１ノードは、第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するＳ５０５。そして、第２アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するＳ５０６。
【選択図】図５



【特許請求の範囲】
【請求項１】
鍵更新方法であって、
第１鍵更新要求を第２ノードへ第１ノードが送信する段階であって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、前記第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、段階と、
第１応答メッセージを前記第２ノードから前記第１ノードが受信する段階であって、前記第１応答メッセージは第２アイデンティティ認証情報を含む、段階と、
前記第１共有鍵を使用することによって、前記第２アイデンティティ認証情報に対する検証を前記第１ノードが実行する段階と、を備え、
前記第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示す
方法。
【請求項２】
前記第１鍵更新要求は第１フレーム番号または第１媒体アクセス制御（ＭＡＣ）シリアル番号を含み、前記第１フレーム番号または前記第１ＭＡＣシリアル番号は前記第１更新時点を示す、請求項１に記載の方法。
【請求項３】
前記第１目標鍵は、前記第１更新時点から開始する前記第１目標鍵の前記有効期間内に適用される、請求項１または２に記載の方法。
【請求項４】
前記第１共有鍵はマスター鍵である、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記第１共有鍵はセッション鍵であり、前記セッション鍵は、マスター鍵に従って鍵導出アルゴリズム（ＫＤＦ）によって生成される、請求項１から４のいずれか一項に記載の方法。
【請求項６】
前記第１鍵ネゴシエーションパラメータはカウンタ値を含み、前記セッション鍵は、前記マスター鍵および前記カウンタ値に従って生成される、請求項５に記載の方法。
【請求項７】
前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、第２目標鍵および前記新規パラメータに基づいて前記第１目標鍵を前記第１ノードが生成する段階を含む、請求項１から６のいずれか一項に記載の方法。
【請求項８】
前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、第２目標鍵、前記新規パラメータおよびアルゴリズム識別子に基づいて前記第１目標鍵を前記第１ノードが生成する段階であって、前記アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムを識別する、段階を含む、請求項１から７のいずれか一項に記載の方法。
【請求項９】
前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つは、前記第２目標鍵に基づいて決定された前記暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、前記第２目標鍵に基づいて決定された前記完全性保護鍵を使用することによって、前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つに対して実行される、請求項８に記載の方法。
【請求項１０】
前記第１鍵更新要求は第１フレーム番号を含み、前記第１フレーム番号は前記第１目標

鍵の更新時点を示し、第１鍵更新要求を第２ノードへ送信する前記段階は、第１通信フレームを使用することによって前記第１鍵更新要求を前記第２ノードへ前記第１ノードが送信する段階であって、前記第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求に保持される第３フレーム番号より小さく、前記第３フレーム番号は、前記前回の更新された鍵の更新時点を示し、前記第１フレーム番号は前記第２フレーム番号より大きく、前記第３フレーム番号より小さい、段階を含み、フレーム番号が大きいほど後の時点を示す、請求項１から９のいずれか一項に記載の方法。

【請求項１１】

前記第１通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む、請求項１０に記載の方法。

【請求項１２】

装置であって、

第１鍵更新要求を第２ノードへ送信するよう構成される送信ユニットであって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、前記第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、送信ユニットと、

第１応答メッセージを前記第２ノードから受信するよう構成される受信ユニットであって、前記第１応答メッセージは第２アイデンティティ認証情報を含む、受信ユニットと、

前記第１共有鍵を使用することによって、前記第２アイデンティティ認証情報に対する検証を実行するよう構成される検証ユニットと、を備え、

前記第１鍵更新要求は第１更新時点および第１目標鍵の有効期間の少なくとも１つを示す

装置。

【請求項１３】

前記第１鍵更新要求は第１フレーム番号または第１媒体アクセス制御（ＭＡＣ）シリアル番号を含み、前記第１フレーム番号または前記第１ＭＡＣシリアル番号は前記第１更新時点を示す、請求項１２に記載の装置。

【請求項１４】

前記第１目標鍵は、前記第１更新時点から開始する前記第１目標鍵の前記有効期間内に適用される、請求項１２または１３に記載の装置。

【請求項１５】

前記第１共有鍵はマスター鍵である、請求項１２から１４のいずれか一項に記載の装置。

【請求項１６】

前記第１共有鍵はセッション鍵であり、前記セッション鍵は、マスター鍵に従って鍵導出アルゴリズム（ＫＤＦ）によって生成される、請求項１２から１５のいずれか一項に記載の装置。

【請求項１７】

前記第１鍵ネゴシエーションパラメータはカウンタ値を含み、前記セッション鍵は、前記マスター鍵および前記カウンタ値に従って生成される、請求項１６に記載の装置。

【請求項１８】

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記装置は、第２目標鍵および前記新規パラメータに基づいて前記第１目標鍵を生成するよう構成される決定ユニットを備える、請求項１２から１７のいずれか一項に記載の装置。

【請求項１９】

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記装置は、第２目標鍵、前記新規パラメータおよびアルゴリズム識別子に基づいて前記第１目標鍵を生成するよう構成される決定ユニットを備え、前記アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムを識別する、請求項１２から１７のい

ずれか一項に記載の装置。
【請求項２０】
前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つは、前記第２目標鍵に基づいて決定された前記暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、前記第２目標鍵に基づいて決定された前記完全性保護鍵を使用することによって、前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つに対して実行される、請求項１９に記載の装置。
【請求項２１】
前記第１鍵更新要求は第１フレーム番号を含み、前記第１フレーム番号は前記第１目標鍵の更新時点を示し、前記送信ユニットは、第１通信フレームを使用することによって前記第１鍵更新要求を前記第２ノードへ送信するよう構成され、前記第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求に保持される第３フレーム番号より小さく、前記第３フレーム番号は、前記前回の更新された鍵の更新時点を示し、前記第１フレーム番号は、前記第２フレーム番号より大きく、前記第３フレーム番号より小さく、フレーム番号が大きいほど後の時点を示す、請求項１２から２０のいずれか一項に記載の装置。
【請求項２２】
前記第１通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む、請求項２１に記載の装置。
【請求項２３】
少なくとも１つのプロセッサおよび通信インタフェースを備える装置であって、前記少なくとも１つのプロセッサは、少なくとも１つのメモリに記憶されたコンピュータプログラムを呼び出すよう構成され、請求項１から１１のいずれか一項に記載の方法を前記装置が実装することを可能にする、装置。
【請求項２４】
１または複数のプロセッサに、請求項１から１１のいずれか一項に記載の方法を実行させる
コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信技術の分野、特に、短距離通信技術、例えば、運転席ドメイン通信の分野に関する。具体的には、本発明は鍵更新方法および関連装置に関する。
【背景技術】
【０００２】
通信技術は人々の生活に浸透している。人々は通信の利便性を享受している一方、セキュリティ上の脆弱性およびプライバシ漏洩の脅威にも直面している。通信プロセスにおけるデータ送信およびストレージのセキュリティを確実にするべく、ノードは通常、データを記憶または送信する前に送信データを暗号化する。受信側のノードはデータを受信した後に、暗号文を解読して平文を復元する。加えて、ノードは更に、データに対して完全性保護（または略して完全性保護）を実行し得る。受信側のノードは、データを受信した後に、メッセージに対して完全性検証を実行する。完全性検証が成功した場合、メッセージが伝送プロセスにおいて修正されていないことを示す。セキュアなデータ通信中に、通信の双方は、暗号化／解読鍵および完全性保護鍵などの鍵を有する必要がある。暗号化／解読鍵および完全性保護鍵などの鍵が失効する、またはクラッキングされると、鍵を使用する暗号化または完全性保護の実行に関する情報が漏洩する可能性が高く、これにより、データ送信セキュリティに影響を及ぼす。
【０００３】
鍵の使用期間は有限である。鍵が公開される、またはクラッキングされることを防止す

るべく、通常は鍵更新の仕組みが使用される。すなわち、鍵の有効期間の終了が近いとき、古い鍵が新しい鍵で置き換えられる。鍵更新プロセスにおいて、鍵更新に使用され、ノードによって送信されるメッセージは中間者攻撃に脆弱であり、これにより、データセキュリティが影響を受ける。

【０００４】

したがって、当業者は、鍵更新プロセスにおいてどのようにデータセキュリティを改善するかという問題を研究している。

【発明の概要】

【０００５】

本願の実施形態は、鍵更新プロセスにおけるデータセキュリティを改善するための鍵更新方法および関連装置を開示する。

【０００６】

第１態様によれば、本願の実施形態は、以下のステップを備える鍵更新方法を開示する。

【０００７】

第１鍵更新要求が第２ノードへ送信され、ここで、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される。第１共有鍵は、通信の双方のノードに記憶される同一の秘密値であり、マスター鍵、セッション鍵、事前共有鍵ＰＳＫまたは同様のものであり得る。セッション鍵は、ノードによって送信されたデータまたはファイルに対する暗号化または完全性保護を実行するために使用され得る。加えて第１アイデンティティ認証情報は、第１共有鍵に基づいて暗号アルゴリズムを使用することによって生成され得る。暗号アルゴリズムは、ハッシュアルゴリズム（ハッシュアルゴリズムとも称される）、認証アルゴリズム、または同様のもの、例えば、ハッシュベースメッセージ認証コードＨＭＡＣアルゴリズム（ＨＭＡＣセキュアハッシュアルゴリズムＨＭＡＣ－ＳＨＡ２５６、ＨＭＡＣ－ＳＨＡ３、ＨＭＡＣ中国暗号アルゴリズムＨＭＡＣ－ＳＭ３などを含む）であり得る。更に、暗号アルゴリズムは、ｃＤＮＡ末端高速増幅ＲＡＣＥ完全性プリミティブ評価メッセージダイジェストＲＩＰＥＭＤアルゴリズムを更に含み得る。

【０００８】

第１応答メッセージが第２ノードから受信され、ここで、第１応答メッセージは第２アイデンティティ認証情報を含む。第２アイデンティティ認証情報を生成する原則は、第１アイデンティティ認証情報の原則と同一であり、詳細は本明細書において改めて説明されない。

【０００９】

第１共有鍵を使用することによって、第２アイデンティティ認証情報に対して検証が実行される。

【００１０】

第２アイデンティティ認証情報に対する検証が成功した場合、第１目標鍵が、第１鍵ネゴシエーションパラメータに基づいて決定される。

【００１１】

上述した方法において、元の鍵が失効する前に、第１ノードおよび第２ノードが第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【００１２】

第１態様の可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【００１３】

従来の鍵更新プロセスにおいて、鍵更新時点がプロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願における鍵更新方法において、第１ノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、更新時点および／または有効期間を第２ノードに示し得、その結果、第１目標鍵を適宜に有効化できる。

【００１４】

第１態様の更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。第１鍵更新要求は、第１フレーム番号を使用することによって第１更新時点を示すために使用される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【００１５】

第１態様の更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【００１６】

第１態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することは、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成することを含む。

【００１７】

第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータは、鍵ネゴシエーションプロセスにおいて生成されるアルゴリズムパラメータである。鍵ネゴシエーションは、通信の双方がいくつかのパラメータを交換して、ネゴシエーションを通じて鍵を取得するプロセスである。鍵ネゴシエーションに使用されるアルゴリズムは、鍵ネゴシエーションアルゴリズムまたは鍵交換アルゴリズムと称される。本願の本実施形態において、第１ノードは第１鍵ネゴシエーションアルゴリズムパラメータを生成し、第２ノードは第２鍵ネゴシエーションアルゴリズムパラメータを生成する。第１目標鍵は、双方によって提供される鍵ネゴシエーションアルゴリズムパラメータを使用することによって決定される。ＤＨアルゴリズムを例とすると、２つのノードはそれぞれ、同一の大きい素数ｐおよび同一のジェネレータ数ｇを使用することによって、乱数ａおよびｂを生成する。第１ノードは、ｇのａ乗　ｍｏｄ　Ｐによって生成された値Ａを第２ノードへ送信し、第２ノードは、ｇのｂ乗　ｍｏｄ　Ｐによって生成された値Ｂを第１ノードへ送信し、次に、第１ノードは受信値Ａに対してａ乗演算を実行し、第２ノードは受信値Ｂに対してａ乗演算を実行する。$K=A^b \bmod p=(g^a \bmod p)^b \bmod p=g^{ab} \bmod p=(g^b \bmod p)^a \bmod p=B^a \bmod p$であるので、第１ノードおよび第２ノードによって生成された鍵Ｋは同一である。

【００１８】

第１態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パ

ラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成することを含む。

【００１９】

第２目標鍵は第１ノードと第２ノードとの間で共有される秘密値であり得るか、または、第１ノードと第２ノードとの間の共有鍵と称され得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。

【００２０】

第１態様の更に別の可能な実装において、第１目標鍵はマスター鍵である。

【００２１】

マスター鍵は、ノードの高クラスの秘密値であり、主にセッション鍵などの鍵を保護するために使用される。任意選択の解決策において、セッション鍵は、マスター鍵に基づいて、鍵導出関数（ｋｅｙ　ｄｅｒｉｖａｔｉｏｎ　ｆｕｎｃｔｉｏｎ，　ＫＤＦ）を使用することによって取得される。任意選択で、マスター鍵はセッション鍵を暗号化するために使用され得る。

【００２２】

第１態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することは、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成することを含み、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。

【００２３】

第１態様の更に別の可能な実装において、第１目標鍵は完全性保護鍵または暗号化鍵である。

【００２４】

第１態様の更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定される暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【００２５】

従来の鍵更新方法は古い鍵（すなわち第２目標鍵）が失効するときに鍵を更新することであると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、第１目標鍵は、第２目標鍵が失効する前に決定され得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【００２６】

第１態様の更に別の可能な実装において、第１鍵更新要求を第２ノードへ送信することは、第１通信フレームを使用することによって第１鍵更新要求を第２ノードへ送信することを含み、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用される鍵更新要求に保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵

に基づいて暗号化を実行することであり得る。したがって、フレーム番号が前回更新された鍵のフレーム番号まで繰り返す前に第１目標鍵が決定され、その結果、データフレームが、第１目標鍵を使用することによって暗号化される。このように、同一のフレーム番号を有するデータフレームが、異なる鍵を使用することによって２回暗号化され得、これにより、データセキュリティを改善する。代替的解決策において、第１鍵更新要求は、第１フレーム番号の代わりにＭＡＣシリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮはＭビットを使用することによって示され、Ｍビットは Ｆビットの一部であり、ＭはＦより小さい。代替的に、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号はまた、ＭＡＣ　ＳＮ、すなわち、第３フレーム番号の示すために使用される複数のビットの一部によって示されるＭＡＣ　ＳＮで置き換えられ得る。この代替的解決策において、第１フレーム番号、第２フレーム番号、および第３フレーム番号の間の値関係は変化しないままである。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【００２７】

第１態様の更に別の可能な実装において、通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む。更に、本願におけるフレーム番号は通信フレームのフレーム番号である。

【００２８】

第１態様の更に別の可能な実装において、方法は更に、第２アイデンティティ情報に対する検証が失敗した場合、第２ノードへの通信接続を切断する、または、更新失敗情報を第２ノードへ送信することを含む。

【００２９】

第２アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、第１ノードは、第２ノードへの通信接続を切断し得るか、または、更新失敗情報を第２ノードへ送信し得、その結果、鍵更新を実行する必要があるノードに対するアクセス要求が再初期化され、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【００３０】

第１態様の更に別の可能な実装において、第１共有鍵を使用することによって第２アイデンティティ認証情報に対して検証を実行する前に、方法は更に、第１応答メッセージに対して完全性検証を実行する段階と、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するステップを実行する段階と、完全性検証が失敗した場合、第２ノードへの通信接続を切断する、または、更新失敗情報を第２ノードへ送信する段階とを備える。

【００３１】

上述した方法において、アイデンティティ情報に対する検証を実行する前に、第１ノードはまず、第１応答メッセージに対する完全性検証を実行して、第１応答メッセージにおける情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１応答情報におけるデータは改ざんされ、鍵は更新できないことを示す。したがって、第１ノードは、第２ノードへの通信接続を切断するか、または、更新失敗情報を第２ノードへ送信し、その結果、第１ノードは、鍵更新を実行する必要があるノードに再アクセスし、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【００３２】

第２態様によれば、本願の実施形態は、以下のステップを含む鍵更新方法を開示する。

【００３３】

第１鍵更新要求が第１ノードから受信され、ここで、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む。第１アイデンティティ認証情報は、第１共有鍵に基づいて暗号アルゴリズムを使用することによって生成され得る。暗号アルゴリズムは、ハッシュアルゴリズム（ハッシュアルゴリズムとも称される）、認証アルゴリズム、または同様のもの、例えば、ハッシュベースメッセージ認証コードＨＭＡＣアルゴリズム（ＨＭＡＣセキュアハッシュアルゴリズムＨＭＡＣ－ＳＨＡ２５６、ＨＭＡＣ－ＳＨＡ３、ＨＭＡ中国暗号アルゴリズムＨＭＡＣ－ＳＭ３などを含む）であり得る。更に、暗号アルゴリズムは、ｃＤＮＡ末端高速増幅ＲＡＣＥ完全性プリミティブ評価メッセージダイジェストＲＩＰＥＭＤアルゴリズムを更に含み得る。

【００３４】

第１共有鍵を使用することによって、第１アイデンティティ認証情報に対して検証が実行される。第１共有鍵は、通信の双方のノードに記憶される同一の秘密値であり、マスター鍵、セッション鍵、事前共有鍵ＰＳＫまたは同様のものであり得る。セッション鍵は、ノードによって送信されたデータまたはファイルに対する暗号化または完全性保護を実行するために使用され得る。加えて第１アイデンティティ認証情報は、第１共有鍵に基づいて暗号アルゴリズムを使用することによって生成され得る。したがって、第２ノードは、第１共有鍵に基づいて暗号アルゴリズムを使用することによって、第１アイデンティティ認証情報に対して検証を実行し得る。第１アイデンティティ認証情報に対する検証が成功した場合、第１目標鍵が第１鍵ネゴシエーションパラメータに基づいて決定される。

【００３５】

第１応答メッセージが第１ノードへ送信され、ここで、第１応答メッセージは第２アイデンティティ認証情報を含み、第２アイデンティティ認証情報は第１共有鍵を使用することによって生成される。第２アイデンティティ認証情報を生成する原則は、第１アイデンティティ認証情報の原則と同一であり、詳細は本明細書において改めて説明されない。

【００３６】

上述した方法において、元のセッション鍵が失効する前に、第１ノードおよび第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【００３７】

第２態様の可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【００３８】

従来の鍵更新プロセスにおいて、鍵更新時点がプロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願における鍵更新方法において、第１ノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、更新時点および／または有効期間を第２ノードに示し得、その結果、第１目標鍵を適宜に有効化できる。

【００３９】

第２態様の更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを

示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【００４０】

第２態様の更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【００４１】

第２態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することは、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成することを含む。

【００４２】

第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータは、鍵ネゴシエーションプロセスにおいて生成されるアルゴリズムパラメータである。鍵ネゴシエーションは、通信の双方がいくつかのパラメータを交換して、ネゴシエーションを通じて鍵を取得するプロセスである。鍵ネゴシエーションに使用されるアルゴリズムは、鍵ネゴシエーションアルゴリズムまたは鍵交換アルゴリズムと称される。本願の本実施形態において、第１ノードは第１鍵ネゴシエーションアルゴリズムパラメータを生成し、第２ノードは第２鍵ネゴシエーションアルゴリズムパラメータを生成する。第１目標鍵は、双方によって提供される鍵ネゴシエーションアルゴリズムパラメータを使用することによって決定される。ＤＨアルゴリズムを例とすると、２つのノードはそれぞれ、同一の大きい素数ｐおよび同一のジェネレータ数ｇを使用することによって、乱数ａおよびｂを生成する。第１ノードは、ｇのａ乗 ｍｏｄ Ｐによって生成された値Ａを第２ノードへ送信し、第２ノードは、ｇのｂ乗 ｍｏｄ Ｐによって生成された値Ｂを第１ノードへ送信し、次に、第１ノードは受信値Ａに対してａ乗演算を実行し、第２ノードは受信値Ｂに対してａ乗演算を実行する。$K=A^b \bmod p=(g^a \bmod p)^b \bmod p=g^{ab} \bmod p=(g^b \bmod p)^a \bmod p=B^a \bmod p$であるので、第１ノードおよび第２ノードによって生成された鍵Ｋは同一である。

【００４３】

第２態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成することを含む。

【００４４】

第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ ｎｕｍｂｅｒ）などを含み得る。

【００４５】

第２態様の更に別の可能な実装において、第１目標鍵はマスター鍵である。

【００４６】

マスター鍵は、ノードの高クラスの秘密値であり、主にセッション鍵などの鍵を保護するために使用される。任意選択の解決策において、セッション鍵は、マスター鍵に基づいて、鍵導出関数（ｋｅｙ ｄｅｒｉｖａｔｉｏｎ ｆｕｎｃｔｉｏｎ，ＫＤＦ）を使用

することによって取得される。任意選択で、マスター鍵はセッション鍵を暗号化するために使用され得る。

【００４７】

第２態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することは、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成することを含み、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。

【００４８】

第２態様の更に別の可能な実装において、第１目標鍵は完全性保護鍵または暗号化鍵である。

【００４９】

第２態様の更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定される暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【００５０】

従来の鍵更新方法は、古い鍵（すなわち、第２目標鍵）が失効するときに鍵を更新することであると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、第１目標鍵は、第２目標鍵が失効する前に決定され得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【００５１】

第２態様の更に別の可能な実装において、方法は更に、第１アイデンティティ情報に対する検証が失敗した場合、第１ノードへの接続を切断する、または、更新失敗インジケーション情報を第１ノードへ送信することを含む。

【００５２】

第１アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、第２ノードは第１ノードへの接続を切断するか、または、更新失敗インジケーション情報を第１ノードへ送信し得、現在の鍵プロセスを停止し、これにより、鍵更新プロセスにおける第２ノードのデータセキュリティを確実にする。

【００５３】

第２態様の更に別の可能な実装において、第１共有鍵を使用することによって第１アイデンティティ認証情報に対する検証を実行する前に、方法は更に、第１鍵更新要求に対する完全性検証を実行する段階と、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するステップを実行する段階と、完全性検証が失敗した場合、第１ノードへの接続を切断し、または更新失敗インジケーション情報を第１ノードへ送信する段階とを備える。

【００５４】

上述した方法において、アイデンティティ情報に対する検証を実行する前に、第２ノードはまず、第１鍵更新要求に対する完全性検証を実行して、第１鍵更新要求における情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１鍵更新要求におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、第２ノードは、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【００５５】

第３態様によれば、本願の実施形態は装置を開示し、装置は、第１鍵更新要求を第２ノ

ードへ送信するよう構成される送信ユニットであって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、前記第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、送信ユニットと、第１応答メッセージを前記第２ノードから受信するよう構成される受信ユニットであって、第１応答メッセージは第２アイデンティティ認証情報を含む、受信ユニットと、前記第１共有鍵を使用することによって、前記第２アイデンティティ認証情報に対する検証を実行するよう構成される検証ユニットと、前記第２アイデンティティ認証情報に対する前記検証が成功した場合、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するよう構成される決定ユニットとを備える。

【００５６】

鍵更新プロセスにおいて、上述のノードおよび第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【００５７】

第３態様の可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【００５８】

従来の鍵更新プロセスにおいて、鍵更新時点がプロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願において提供されるノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、第２ノードへの更新時点および／または有効期間を示し得、その結果、第１目標鍵を適宜に有効化することができる。

【００５９】

第３態様の更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【００６０】

第３態様の更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【００６１】

第３態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、決定ユニットは、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。

【００６２】

第３態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは、新規パラメータを含み、決定ユニットは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。

【００６３】
第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。

【００６４】
第３態様の更に別の可能な実装において、第１目標鍵はノードのマスター鍵である。

【００６５】
第３態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、決定ユニットは、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、ここで、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。

【００６６】
第３態様の更に別の可能な実装において、第１目標鍵はノードの完全性保護鍵または暗号化鍵である。

【００６７】
第３態様の更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定される暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【００６８】
従来の鍵更新方法は、古い鍵が失効するときに鍵を更新することであると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において提供されるノードは、鍵が失効する前に第１目標鍵を決定し得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【００６９】
第３態様の更に別の可能な実装において、送信ユニットは、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信するよう構成され、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。

【００７０】
通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行することであり得る。したがって、フレーム番号が前回更新された鍵のフレーム番号まで繰り返す前に第１目標鍵が決定され、その結果、データフレームが、第１目標鍵を使用することによって暗号化される。このように、同一のフレーム番号を有するデータフレームが、異なる鍵を使用することによって２回暗号化され得、これにより、データセキュリティを改善する。代替的解決策において、第１鍵更新要求は、第１フレーム番号の代わりにＭＡＣシリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮはＭビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。代替的に、前回の鍵更

新中に使用される鍵更新要求において保持される第３フレーム番号はまた、ＭＡＣ　ＳＮ、すなわち、第３フレーム番号の示すために使用される複数のビットの一部によって示されるＭＡＣ　ＳＮで置き換えられ得る。この代替的解決策において、第１フレーム番号、第２フレーム番号、および第３フレーム番号の間の値関係は変化しないままである。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【００７１】

第３態様の更に別の可能な実装において、通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む。

【００７２】

第３態様の更に別の可能な実装において、第２アイデンティティ情報に対する検証が失敗した場合、送信ユニットおよび受信ユニットは第２ノードへの通信接続を切断するか、または、更新失敗情報を第２ノードへ送信する。

【００７３】

第２アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、上述のノードは、第２ノードへの通信接続を切断し得るか、または、更新失敗情報を第２ノードへ送信し得、その結果、鍵更新を実行する必要があるノードに対するアクセス要求が再初期化され、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【００７４】

第３態様の更に別の可能な実装において、検証ユニットは更に、第１応答メッセージに対する完全性検証を実行するよう構成され、完全性検証が成功した場合、続いて、第１共有鍵を使用することによって、第２アイデンティティ認証情報に対する検証を実行するステップを実行し、完全性検証が失敗した場合、送信ユニットおよび受信ユニットは第２ノードへの通信接続を切断するか、または、送信ユニットを使用することによって、更新失敗情報を第２ノードへ送信するか、もしくは、更新失敗情報を第２ノードへ送信し得る。

【００７５】

ノードは、アイデンティティ情報に対する検証を実行する前に、まず、第１応答メッセージに対する完全性検証を実行し、第１応答メッセージにおける情報が改ざんされていないと決定し得る。完全性検証が失敗した場合、第１応答情報におけるデータは改ざんされ、鍵は更新できないことを示す。したがって、ノードは、第２ノードへの通信接続を切断するか、または、更新失敗情報を第２ノードへ送信し、その結果、ノードは、鍵更新を実行する必要があるノードに再アクセスし、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【００７６】

第４態様によれば、本願の実施形態は装置を開示し、装置は、第１鍵更新要求を第１ノードから受信するよう構成される受信ユニットであって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む、受信ユニットと、第１共有鍵を使用することによって前記第１アイデンティティ認証情報に対する検証を実行するよう構成される検証ユニットと、前記第１アイデンティティ認証情報に対する前記検証が成功した場合、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するよう構成される決定ユニットと、第１応答メッセージを前記第１ノードへ送信するよう構成される送信ユニットであって、前記第１応答メッセージは第２アイデンティティ認証情報を含み、前記第２アイデンティティ認証情報は、前記第１共有鍵を使用することによって生成される、送信ユニットとを備える。

【００７７】
元のセッション鍵が失効する前に、上述のノードおよび第１ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。
【００７８】
第４態様の可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。
【００７９】
従来の鍵更新プロセスにおいて、鍵更新時点がプロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願における鍵更新方法において、第１ノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、更新時点および／または有効期間をノードに示し得、その結果、第１目標鍵を適宜に有効化できる。
【００８０】
第４態様の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は、第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。
【００８１】
第４態様の更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。
【００８２】
第４態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、決定ユニットは、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。
【００８３】
第４態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは、新規パラメータを含み、決定ユニットは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。
【００８４】
第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）な

どを含み得る。

【００８５】

第４態様の更に別の可能な実装において、第１目標鍵はノードのマスター鍵である。

【００８６】

第４態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、決定ユニットは、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、ここで、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムを識別するために使用される。

【００８７】

第４態様の更に別の可能な実装において、第１目標鍵は、第２ノードの完全性保護鍵または暗号化鍵である。第４態様の更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定される暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【００８８】

従来の鍵更新方法は、古い鍵が失効するとき、鍵を更新するものと理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、第１目標鍵は、鍵が失効する前に決定され得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【００８９】

第４態様の更に別の可能な実装において、第１アイデンティティ情報に対する検証が失敗した場合、送信ユニットおよび受信ユニットは、第１ノードへの接続を切断するか、または、送信ユニットを使用することによって更新失敗インジケーション情報を第１ノードへ送信する。

【００９０】

第１アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、ノードは第１ノードへの接続を切断するか、または、更新失敗インジケーション情報を第１ノードへ送信し得、現在の鍵プロセスを停止し、これにより、鍵更新プロセスにおけるノードのデータセキュリティを確実にする。

【００９１】

第４態様の更に別の可能な実装において、検証ユニットは更に、第１鍵更新要求に対する完全性検証を実行するよう構成され、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するステップを実行し、完全性検証が失敗した場合、ノードは第１ノードへの接続を切断するか、または、送信ユニットを使用することによって更新失敗インジケーション情報を第１ノードへ送信する。

【００９２】

上述のノードは、アイデンティティ情報に対する検証を実行する前に、まず第１鍵更新要求に対する完全性検証を実行して、第１鍵更新要求における情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１鍵更新要求におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、上述のノードは、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【００９３】

第５態様によれば、本願の実施形態は装置を開示する。ノードはメモリ、プロセッサお

よび通信インタフェースを備え、メモリは計算機プログラムを記憶し、プロセッサは、メモリに記憶されたコンピュータプログラムを呼び出し、以下のオペレーション、すなわち、通信インタフェースを通じて第１鍵更新要求を第２ノードへ送信することであって、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、こと、通信インタフェースを通じて、第１応答メッセージを第２ノードから受信することであって、第１応答メッセージは第２アイデンティティ認証情報を含む、こと、第１共有鍵を使用することによって、第２アイデンティティ認証情報に対する検証を実行すること、および、第２アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することを実行する。

【００９４】

鍵更新プロセスにおいて、上述のノードおよび第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【００９５】

第５態様の可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【００９６】

従来の鍵更新プロセスにおいて、鍵更新時点がプロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願において提供されるノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、第２ノードへの更新時点および／または有効期間を示し得、その結果、第１目標鍵を適宜に有効化することができる。

【００９７】

第５態様の更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【００９８】

第５態様の更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【００９９】

第５態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサは具体的には、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。

【０１００】

第５態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パ

ラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサは具体的には、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。

【０１０１】

第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。

【０１０２】

第５態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサは具体的には、以下のように構成される。

【０１０３】

第５態様の更に別の可能な実装において、第１目標鍵は、ノードのマスター鍵である。第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成し、ここで、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。

【０１０４】

第５態様の更に別の可能な実装において、第１目標鍵は、ノードの完全性保護鍵または暗号化鍵である。

【０１０５】

第５態様の更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定される暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【０１０６】

従来の鍵更新方法は、古い鍵が失効するとき鍵を更新すると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、第１目標鍵は、鍵が失効する前に決定され得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【０１０７】

第５態様の更に別の可能な実装において、通信インタフェースは、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信し、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。

【０１０８】

通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行することであり得る。したがって、フレーム番号が前回更新された鍵のフレーム番号まで繰り返す前に第１目標鍵が決定され、その結果、データフレームが、第１目標鍵を使用することによって暗号化される。このように、同一のフレーム番号を有するデータフレームが、

異なる鍵を使用することによって２回暗号化され得、これにより、データセキュリティを改善する。代替的解決策において、第１鍵更新要求は、第１フレーム番号の代わりにＭＡＣシリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮはＭビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。代替的に、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号はまた、ＭＡＣ　ＳＮ、すなわち、第３フレーム番号の示すために使用される複数のビットの一部によって示されるＭＡＣ　ＳＮで置き換えられ得る。この代替的解決策において、第１フレーム番号、第２フレーム番号、および第３フレーム番号の間の値関係は変化しないままである。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０１０９】

第５態様の更に別の可能な実装において、通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む。

【０１１０】

第５態様の更に別の可能な実装において、プロセッサは更に、第２アイデンティティ情報に対する検証が失敗した場合、第２ノードへの通信接続を切断し、または、通信インタフェースを通じて更新失敗情報を第２ノードへ送信するよう通信インタフェースに示すよう構成される。

【０１１１】

第２アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、上述のノードは、第２ノードへの通信接続を切断し得るか、または、更新失敗情報を第２ノードへ送信し得、その結果、鍵更新を実行する必要があるノードに対するアクセス要求が再初期化され、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０１１２】

第５態様の更に別の可能な実装において、プロセッサは更に、第２ノードから第１応答メッセージを受信した後に、第１応答メッセージに対する完全性検証を実行し、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するステップを実行するよう構成され、プロセッサは更に、完全性検証が失敗した場合、第２ノードへの通信接続を切断するか、または、通信インタフェースを通じて更新失敗情報を第２ノードへ送信するよう通信インタフェースに示すよう構成される。

【０１１３】

完全性検証は、情報が改ざんされているかどうかを決定するために実行され得ることが分かり得る。したがって、アイデンティティ情報に対する検証を実行する前に、上述のノードはまず、第１応答メッセージに対する完全性検証を実行して、第１応答メッセージにおける情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１応答情報におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、ノードは、第２ノードへの通信接続を切断するか、または、更新失敗情報を第２ノードへ送信し、その結果、ノードは、鍵更新を実行する必要があるノードに再アクセスし、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０１１４】

第６態様によれば、本願の実施形態は装置を開示する。ノードはメモリ、プロセッサおよび通信インタフェースを備え、メモリは計算機プログラムを記憶し、プロセッサは、メモリに記憶されたコンピュータプログラムを呼び出し、以下のオペレーション、すなわち

、通信インタフェースを通じて第１鍵更新要求を第２ノードへ送信することであって、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、こと、通信インタフェースを通じて、第１応答メッセージを第２ノードから受信することであって、第１応答メッセージは第２アイデンティティ認証情報を含む、こと、第１共有鍵を使用することによって、第２アイデンティティ認証情報に対する検証を実行すること、および、第２アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することを実行するよう構成される。

【０１１５】

元のセッション鍵が失効する前に、上述のノードおよび第１ノードは第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０１１６】

第６態様の可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【０１１７】

従来の鍵更新プロセスにおいて、鍵更新時点は、プロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願において、第１ノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、更新時点および／または有効期間をノード示し得、その結果、第１目標鍵を適宜に有効化できる。

【０１１８】

第６態様の更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０１１９】

第６態様の更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【０１２０】

第６態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサは具体的には、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。

【０１２１】

第６態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パ

ラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサは具体的には、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。

【０１２２】

第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。

【０１２３】

第６態様の更に別の可能な実装において、第１目標鍵はノードのマスター鍵である。

【０１２４】

第６態様の更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサは具体的には、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。

【０１２５】

第６態様の更に別の可能な実装において、第１目標鍵は、ノードの完全性保護鍵または暗号化鍵である。

【０１２６】

第６態様の更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定される暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【０１２７】

従来の鍵更新方法は、古い鍵が失効するときに鍵を更新することであることが理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、第１目標鍵は、鍵が失効する前に決定され得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【０１２８】

第６態様の更に別の可能な実装において、プロセッサは更に、第１アイデンティティ情報に対する検証が失敗した場合に、第１ノードへの通信接続を切断する、または、通信インタフェースを通じて更新失敗インジケーション情報を第１ノードへ送信するよう通信インタフェースに示すよう構成される。

【０１２９】

第１アイデンティティ認証情報に対する検証が失敗した場合、ノードは、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、現在の鍵プロセスを停止し、これにより、鍵更新プロセスのノードのデータセキュリティを確実にすることが分かり得る。

【０１３０】

第６態様の更に別の可能な実装において、プロセッサは更に、第１鍵更新要求を第１ノードから受信した後、第１鍵更新要求に対する完全性検証を実行し、完全性検証が成功し

た場合、続いて第１共有鍵を使用することによって第１アイデンティティ認証情報に対する検証を実行するステップを実行するよう構成され、プロセッサは更に、完全性検証が失敗した場合、第１ノードへの接続を切断するか、または、通信インタフェースを通じて更新失敗インジケーション情報を第１ノードへ送信するよう通信インタフェースに示すよう構成される。

【０１３１】

上述のノードは、アイデンティティ情報に対する検証を実行する前に、まず第１鍵更新要求に対する完全性検証を実行して、第１鍵更新要求における情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１鍵更新要求におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、上述のノードは、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０１３２】

第７態様によれば、本願の実施形態はコンピュータ可読記憶媒体を開示する。このコンピュータ可読記憶媒体は、コンピュータプログラムを記憶する。コンピュータプログラムが１または複数のプロセッサ上で実行されるとき、第１態様および第１態様の可能な実装のいずれか１つ、または、第２態様および第２態様の可能な実装のいずれか１つにおける方法が実行される。

【０１３３】

第８態様によれば、本願の実施形態はチップシステムを開示する。チップシステムは、少なくとも１つのプロセッサ、メモリおよびインタフェース回路を含む。インタフェース回路は、少なくとも１つのプロセッサについての情報入力／出力を提供するよう構成され、少なくとも１つのメモリはコンピュータプログラムを記憶し、コンピュータプログラムが１または複数のプロセッサで実行されるとき、第１態様および第１態様の可能な実装のいずれか１つ、または、第２態様および第２態様の可能な実装のいずれか１つにおける方法が実行される。

【０１３４】

第９態様によれば、本願の実施形態は車両を開示する。車両は第１ノード（例えば、自動車運転席ドメインコントローラＣＤＣ）を含む。更に、車両は第２ノード（例えば、カメラ、スクリーン、マイク、スピーカ、レーダ、電子鍵、およびキーレスエントリ、または起動システムコントローラなどのモジュールの少なくとも１つ）を更に含む。第１ノードは、第３態様および第３態様の可能な実装のいずれか１つ、または、第５態様および第５態様の可能な実装のいずれか１つにおけるノードであり、第２ノードは、第４態様および第４態様の可能な実装のいずれか１つ、または、第６態様および第６態様の可能な実装のいずれか１つにおけるノードである。

【図面の簡単な説明】

【０１３５】

以下で、本願の実施形態で使用される添付図面を説明する。

【０１３６】

【図１】本願の実施形態によるＤＨアルゴリズムの概略原理図である。

【０１３７】

【図２】本願の実施形態による鍵導出アルゴリズムの概略図である。

【０１３８】

【図３】本願の実施形態による通信システムの概略アーキテクチャ図である。

【０１３９】

【図４】本願の実施形態による鍵更新方法の使用シナリオの概略図である。

【０１４０】

【図５】本願の実施形態による鍵更新方法の概略フローチャートである。

【０１４１】

【図６Ａ】本願の実施形態による更に別の鍵更新方法の概略フローチャートである。

【図６Ｂ】本願の実施形態による更に別の鍵更新方法の概略フローチャートである。
【０１４２】
【図７Ａ】本願の実施形態による更に別の鍵更新方法の概略フローチャートである。
【図７Ｂ】本願の実施形態による更に別の鍵更新方法の概略フローチャートである。
【０１４３】
【図８Ａ】本願の実施形態による更に別の鍵更新方法の概略フローチャートである。
【図８Ｂ】本願の実施形態による更に別の鍵更新方法の概略フローチャートである。
【０１４４】
【図９】本願の実施形態によるノードの概略構造図である。
【０１４５】
【図１０】本願の実施形態による更に別のノードの概略構造図である。
【０１４６】
【図１１】本願の実施形態による更に別のノードの概略構造図である。
【０１４７】
【図１２】本願の実施形態による更に別のノードの概略構造図である。
【発明を実施するための形態】
【０１４８】
以下では、本願の実施形態における添付図面を参照して、本願の実施形態を説明する。本願において、「例」、「例えば」または同様のものなどの単語は、例、例示または説明を提供することを表すために使用されることに留意されたい。本願において「例」または「例えば」として説明される任意の実施形態または設計解決策は、別の実施形態または設計解決策より好ましい、または、より多くの利点を有するものとして説明されるものではない。厳密には、「例」、「例えば」、または同様のものなどの単語の使用は、特定の方式における相対的な概念を提示することを意図する。
【０１４９】
以下ではまず、理解を容易にするために、本願における関連技術および技術用語を簡潔に説明する。
【０１５０】
１．ノード（ｎｏｄｅ）
【０１５１】
ノードとは、データ受信／送信能力を有する電子デバイスである。例えば、ノードは、自動車運転席（Ｃｏｃｋｐｉｔ　Ｄｏｍａｉｎ）デバイス、または、自動車運転席デバイスにおけるモジュール（運転席ドメインコントローラ（ｃｏｃｋｐｉｔ　ｄｏｍａｉｎ　ｃｏｎｔｒｏｌｌｅｒ，　ＣＤＣ）、カメラ、スクリーン、マイク、スピーカ、電子鍵、およびキーレスエントリ、または、起動システムコントローラなどのモジュールの１または複数）であり得る。具体的な実装プロセスにおいて、ノードは、データ転送デバイス、例えば、ルータ、リピータ、ブリッジまたはスイッチであり得るか、または、例えば、ユーザ機器（ｕｓｅｒ　ｅｑｕｉｐｍｅｎｔ、ＵＥ）、携帯電話（ｍｏｂｉｌｅ　ｐｈｏｎｅ）、タブレットコンピュータ（ｐａｄ）、デスクトップコンピュータ、ヘッドセット、およびスピーカなどの様々なタイプの端末デバイスであり得、自動運転（ｓｅｌｆ－ｄｒｉｖｉｎｇ）デバイス、交通安全（ｔｒａｎｓｐｏｒｔａｔｉｏｎ　ｓａｆｅｔｙ）デバイス、仮想現実（ｖｉｒｔｕａｌ　ｒｅａｌｉｔｙ，　ＶＲ）端末デバイス、拡張現実（ａｕｇｍｅｎｔｅｄ　ｒｅａｌｉｔｙ，　ＡＲ）端末デバイス、マシンタイプ通信（ｍａｃｈｉｎｅ　ｔｙｐｅ　ｃｏｍｍｕｎｉｃａｔｉｏｎ，　ＭＴＣ）デバイス、産業用制御（ｉｎｄｕｓｔｒｉａｌ　ｃｏｎｔｒｏｌ）デバイス、リモート医療（ｒｅｍｏｔｅ　ｍｅｄｉｃａｌ）デバイス、スマートグリッド（ｓｍａｒｔ　ｇｒｉｄ）デバイス、およびスマートシティ（ｓｍａｒｔ　ｃｉｔｙ）デバイスなどのマシンインテリジェンスデバイスを更に含み得、ウェアラブルデバイス（例えば、スマートウォッチ、スマートバンド、または歩数計）などを更に含み得る。いくつかの技術シナリオにおいて、同様のデータ受信／送信能力を有するデバイスの名称は、ノードと称されないことがあり得る。しかしな

がら、説明を容易にするべく、データ受信／送信能力を有する電子デバイスは、本願の実施形態において、ノードと総称される。

【０１５２】

２．鍵（ｋｅｙ）

【０１５３】

通信プロセスにおいて、データが通信ノード間で送信される。データを機密に維持する必要がある場合、鍵を使用することによってデータを暗号化する必要がある。ノードにおける機密に維持される必要がある内容の秘密レベルおよび秘密クラスは異なることがあるので、異なるタイプの鍵を暗号化に使用する必要がある。一般的な鍵タイプとして、セッション鍵、マスター鍵、共有鍵などが挙げられる。

【０１５４】

（１）セッション鍵（ｓｅｓｓｉｏｎ　ｋｅｙ）

【０１５５】

セッション鍵として、暗号化鍵、完全性保護鍵、ファイル鍵などが挙げられる。暗号化鍵は、ノードによって送信されるデータを保護するために使用され得、データ暗号化鍵とも称され得る。完全性保護鍵は、送信データに対して完全性保護を実行するために使用され得る。ファイル鍵は、送信ファイルを保護するために使用され得る。任意選択で、セッション鍵は、通信の双方のノードにおいて事前構成され得るか、または、通信の双方の間のネゴシエーションを通じて取得され得るか、または、元の鍵を使用することによって導出され得るか、または、鍵配布センター（Ｋｅｙ　Ｄｉｓｔｒｉｂｕｔｉｏｎ　Ｃｅｎｔｅｒ，　ＫＤＣ）によって割り当てられ得る。任意選択で、セッション鍵は、対称暗号化アルゴリズム（ｓｙｍｍｅｔｒｉｃ　ｅｎｃｒｙｐｔｉｏｎ　ａｌｇｏｒｉｔｈｍ）の鍵であり得るか、または、非対称暗号化アルゴリズム（ａｓｙｍｍｅｔｒｉｃ　ｅｎｃｒｙｐｔｉｏｎ　ａｌｇｏｒｉｔｈｍ）の鍵であり得る。

【０１５６】

（２）マスター鍵（ｍａｓｔｅｒ　ｋｅｙ）

【０１５７】

マスター鍵は、ノードの高クラス秘密値であり、セッション鍵、サブマスター鍵などを導出するために使用され得る。サブマスター鍵は、クラスがマスター鍵とセッション鍵との間の鍵であり、中間鍵と称されることがある。

【０１５８】

いくつかの可能な解決策において、マスター鍵は、物理的または電子的隔離を通じて厳格に保護され得る。

【０１５９】

（３）共有鍵（ｓｈａｒｅｄ　ｋｅｙ，　ＳＫ）

【０１６０】

共有鍵は、通信の双方のノードに記憶される同一の秘密値である。いくつかの任意選択の解決策において、ノードは、マスター鍵、セッション鍵、または事前共有鍵（ｐｒｅ－ｓｈａｒｅｄ　ｋｅｙ，　ＰＳＫ）を共有鍵として使用し得る。ノードには１または複数の共有鍵があり得る。

【０１６１】

例えば、ノードは、セッション鍵を共有鍵として使用する。例えば、ノードＡおよびノードＢが、対称暗号化アルゴリズム（すなわち、同一の鍵が暗号化および解読に使用される）を使用して互いに通信する場合、ノードＡは、暗号化鍵Ｋｍを使用することによって平文メッセージを暗号化し、平文メッセージをノードＢへ送信し、ノードＢは解読鍵Ｋｍを使用することによって平文メッセージを解読する。この場合、暗号化鍵Ｋｍは、２つのノード間の共有鍵として使用され得る。

【０１６２】

別の例として、ノードは、事前共有鍵を共有鍵として使用し得、事前共有鍵は、２つのノード間の接続を識別する秘密値である。事前共有鍵は、通信の双方のノードにおいて事

前構成され得る。例えば、車両の運転席ドメインコントローラ（ｃｏｃｋｐｉｔ　ｄｏｍａｉｎ　ｃｏｎｔｒｏｌｌｅｒ，　ＣＤＣ）および車内レーダデバイスは、互いに通信し得る２つのノードであり、展開中に秘密値がＣＤＣおよび車内レーダについて事前構成され、車両のＣＤＣのみがルーフレーダに接続され得るか、または、データをルーフレーダへ送信し得る。事前共有鍵は代替的に、通信を通じて通信の双方によって取得され得る。例えば、ＣＤＣがＢｌｕｅｔｏｏｔｈ（登録商標）を通じて携帯電話に接続される前に、ペアリングを確認することによって事前共有鍵が生成され得る。加えて、事前共有鍵は、信頼済みデバイス（例えばＫＤＣ）によって別個に第１ノードおよび第２ノードへ送信され得る。

【０１６３】

３．鍵ネゴシエーション

【０１６４】

鍵ネゴシエーションとは、通信の双方がいくつかのパラメータを交換して、ネゴシエーションを通じて鍵を取得するプロセスである。鍵ネゴシエーションに使用されるアルゴリズムは、鍵ネゴシエーションアルゴリズムまたは鍵交換アルゴリズムと称される。一般的な鍵ネゴシエーションアルゴリズムとして、ディフィー・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ，　ＤＨ）アルゴリズム、楕円曲線暗号（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｃｒｙｐｔｏｓｙｓｔｅｍｓ，　ＥＣＣ）ディフィー・ヘルマン（ＥＣＤＨ）アルゴリズム、オークリー（Ｏａｋｌｅｙ）アルゴリズム、中国暗号アルゴリズム（例えば、ＳＭ１、ＳＭ２、ＳＭ３、およびＳＭ４）などが挙げられる。

【０１６５】

ＤＨアルゴリズムを例とすると、２つのノードはそれぞれ、同一の素数ｐおよび同一の乱数ｇを使用することによって、乱数ａおよびｂを生成する。第１ノードは、ｇのａ乗ｍｏｄ　Ｐによって生成された値を第２ノードへ送信し、第２ノードは、ｇのｂ乗ｍｏｄ　Ｐによって生成された値を第１ノードへ送信し、次に、第１ノードは、受信した結果に対してａ乗演算を実行し、第２ノードは、受信した結果に対してａ乗演算を実行し、ここで、ｍｏｄは剰余演算を表す。最後に、パスワードが形成され、鍵交換が完了する。

【０１６６】

図１は、本願の実施形態によるＤＨアルゴリズムの概略原理図である。ＤＨアルゴリズムにおいて鍵を交換するステップは以下の通りである。

【０１６７】

ステップ１：第１ノードが素数ｐ、乱数ｇおよび乱数ａを決定する。

【０１６８】

ステップ２：第１ノードが第１計算値Ａを生成し、Ａは以下の式、すなわち、$A = g^a \bmod p$を満たす。

【０１６９】

ステップ３：第１ノードが素数ｐ、乱数ｇ、および第１計算値Ａを第２ノードへ送信する。

【０１７０】

ステップ４：第２ノードが乱数ｂを決定する。

【０１７１】

ステップ５：第２ノードが計算を通じて第２計算値Ｂを取得し、Ｂは例えば、以下の式、すなわち、$B = g^b \bmod p$を満たす。

【０１７２】

ステップ６：第２ノードがネゴシエーションを通じて鍵$s = A^b \bmod p$を計算する。

【０１７３】

ステップ７：第２ノードが第１計算値Ｂを第１ノードへ送信する。

【０１７４】

ステップ８：第１ノードが$s = B^a \bmod p$を計算する。

【０１７５】
Ｋ＝Ａ^{b} ｍｏｄ ｐ＝（ｇ^{a} ｍｏｄ ｐ）^{b} ｍｏｄ ｐ＝ｇ^{ab} ｍｏｄ ｐ＝（ｇ^{b} ｍｏｄ ｐ）^{a} ｍｏｄ ｐ＝Ｂ^{a} ｍｏｄ ｐなので、第１ノードおよび第２ノードによって計算される鍵ｓは同一である。加えて、鍵ｓはネットワーク上で送信されず、アルゴリズムにおいて選択される素数ｐ、乱数ｇ、乱数ａおよび乱数ｂの値は実際には非常に大きいので、ネットワーク上で送信される素数ｐ、乱数ｇ、第１計算値Ａ、および第２計算値Ｂに基づいて鍵ｓを導出することは困難である。したがって、ＤＨアルゴリズムを使用することによって取得された鍵はセキュアである。

【０１７６】
４．鍵導出

【０１７７】
鍵導出とは、１つの秘密値から１または複数の鍵を導出することである。鍵を導出するのに使用されるアルゴリズムは、鍵導出アルゴリズム（ｋｅｙ ｄｅｒｉｖａｔｉｏｎ ｆｕｎｃｔｉｏｎ，ＫＤＦ）と称される。例えば、秘密値Ｋｅｙを使用することによって導出される新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータ（ｆｒｅｓｈ ｐａｒａｍｅｔｅｒ）であり、更新において使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ ｎｕｍｂｅｒ）などのうち少なくとも１つを含み得る。異なる瞬間の新規パラメータは通常異なる。フレーム番号は、フレームの番号であり、フレームは、複数のビットまたはフィールドを含む特定の情報構造である。例えば、時分割多元接続（ｔｉｍｅ ｄｉｖｉｓｉｏｎ ｍｕｌｔｉｐｌｅ ａｃｃｅｓｓ，ＴＤＭＡ）通信技術において、時間は周期的フレームにセグメント化され、各フレームのフレーム番号は、０から２７１５６４７まで周期的に変化する。

【０１７８】
一般的な鍵導出アルゴリズムとして、パスワードベース鍵導出関数（ｐａｓｓｗｏｒｄ－ｂａｓｅｄ ｋｅｙ ｄｅｒｉｖａｔｉｏｎ ｆｕｎｃｔｉｏｎ，ＰＢＫＤＦ）、スクリプト（ｓｃｒｙｐｔ）アルゴリズムなどが挙げられる。ＰＢＫＤＦアルゴリズムは更に、第１世代ＰＢＫＤＦ１および第２世代ＰＢＫＤＦ２を含む。任意選択で、いくつかのＫＤＦアルゴリズムの鍵導出プロセスにおいて、入力された秘密値に対してハッシュ変更を実行するためにハッシュアルゴリズムが使用される。したがって、アルゴリズム識別子は更に、ＫＤＦ機能における入力として受信され得、使用されるハッシュアルゴリズムを示す。

【０１７９】
ＰＢＫＤＦ２を例とすると、ＰＢＫＤＦ２アルゴリズムにおいて秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＰＢＫＤＦ２（ＰＲＦ、Ｋｅｙ、ｓａｌｔ、ｃ、ｄｋ＿ｌｅｎ）として表現され得、ここで、パラメータＰＲＦは、使用されるハッシュアルゴリズムの識別子を示し、ｓａｌｔは、ランダムに生成されるソルトであり、新規パラメータとみなされ得、ｃは反復回数の量であり、ｄｋ＿ｌｅｎは、生成されたＤＫの長さであり、ブロックサイズとも称され得、デフォルトであり得る。図２は、本願の実施形態による鍵導出アルゴリズムの概略図である。導出された鍵１は、秘密値２０１、アルゴリズム識別子１、および新規パラメータｆｒｅｓｈ１を使用することによって取得され得、導出された鍵２は、秘密値２０１、アルゴリズム識別子１、および新規パラメータｆｒｅｓｈ２を使用することによって取得され得、ここで、反復回数の量およびブロックサイズは事前設定される。

【０１８０】
５．暗号アルゴリズム

【０１８１】
暗号アルゴリズムは、暗号化および／または解読のための数学的関数であり得、暗号関数とも称され得る。一般的な暗号アルゴリズムとして、ハッシュアルゴリズム、認証アル

ゴリズム、または同様のものが挙げられる。ハッシュアルゴリズムは、ハッシュ（Ｈａｓｈ）関数またはハッシュアルゴリズムとも称される。ハッシュアルゴリズムは、任意の長さの情報を識別子に変換するために使用され得、逆のルールを発見することは困難である。一般的なハッシュアルゴリズムとして、ハッシュベースメッセージ認証コード（ｈａｓｈ－ｂａｓｅｄ ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ，ＨＭＡＣ）、ＨＭＡＣ中国暗号アルゴリズムＨＭＡＣ－ＳＭ（例えば、ＨＭＡＣ－ＳＭ３）、ＨＭＡＣ－ＳＨＡ２５６またはＨＭＡＣ－ＳＨＡ３などのＨＭＡＣセキュアハッシュアルゴリズム（ＨＭＡＣセキュアハッシュアルゴリズム、ＨＭＡＣ－ＳＨＡ）などが挙げられ、ＭＤ２、ＭＤ４、またはＭＤ５などのメッセージダイジェスト（ｍｅｓｓａｇｅ ｄｉｇｅｓｔ，ＭＤ）アルゴリズムを更に含み得る。更に、暗号アルゴリズムは、ｃＤＮＡ末端の高速増幅（ｒａｐｉｄ－ａｍｐｌｉｆｉｃａｔｉｏｎ ｏｆ ｃＤＮＡ ｅｎｄｓ，ＲＡＣＥ）完全性プリミティブ評価メッセージダイジェスト（ＲＡＣＥ Ｉｎｔｅｇｒｉｔｙ Ｐｒｉｍｉｔｉｖｅｓ Ｅｖａｌｕａｔｉｏｎ Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ，ＲＩＰＥＭＤ）アルゴリズムを更に含み得る。

【０１８２】

以下では、本願の実施形態におけるシステムアーキテクチャおよびサービスシナリオを説明する。本願において説明されるシステムアーキテクチャおよびサービスシナリオは、本願における技術的解決策をより明確に説明することを意図するものであり、本願において提供される技術的解決策に対する限定を構成するものではないことに留意されたい。当業者であれば、システムアーキテクチャの発展および新しいサービスシナリオの登場に伴い、本願において提供される技術的解決策は、同様の技術的問題にも適用可能であることに気付き得る。

【０１８３】

図３は、本願の実施形態による通信システムの概略アーキテクチャ図である。通信システムは、第１ノード３０１および第２ノード３０２を備える。第１ノード３０１は、データリンクを通じて第２ノード３０２と通信し得る。盗聴者（または攻撃者）が情報の内容を取得することを防止するべく、通信中の情報は、暗号化鍵を使用することによって暗号化され得る。例えば、第１ノード３０１は、暗号化鍵３０５を使用することによって、送信される必要がある平文メッセージ３０３を暗号化し、暗号文メッセージ３０４を取得する。第１ノード３０１は、暗号文メッセージ３０４を第２ノード３０２へ送信する。それに対応して、第２ノード３０２は、暗号文メッセージ３０４を受信した後に、鍵を使用することによって暗号文メッセージ３０４を解読して平文メッセージ３０３を取得し得、これにより、データ送信を完了する。暗号化鍵および解読鍵に加えて、第１ノード３０１および第２ノード３０２は更に、完全性保護鍵、ファイル鍵、およびマスター鍵などの鍵を含み得る。

【０１８４】

第１ノード３０１および第２ノード３０２は異なるデバイスであり得ることに留意されたい。例えば、図４は、本願の実施形態による鍵更新方法の使用シナリオの概略図である。ＣＤＣ４０１およびカメラ４０２は、スマート運転席デバイスにおける２つのノードである。ＣＤＣ４０１は第１ノード３０１とみなされ得、カメラ４０２は第２ノード３０２とみなされ得る。カメラ４０２は、鍵を使用することによってビデオデータを暗号化し、Ｂｌｕｅｔｏｏｔｈを通じて暗号化ビデオデータをＣＤＣ４０１へ送信し、ＣＤＣ４０１はＢｌｕｅｔｏｏｔｈを通じて暗号化ビデオデータを受信し、暗号化ビデオデータを解読して、撮影されたビデオデータを取得する。第１ノード３０１および第２ノード３０２は代替的に、同一のタイプのノードであり得る。例えば、第１ノード３０１が携帯電話Ａであり、かつ、第２ノード３０２が携帯電話Ｂである場合、携帯電話Ａは、ローカル音声データを暗号化し、ネットワークコールを通じて、暗号化された音声データをＢ側へ送信し得る。

【０１８５】

任意選択で、第１ノード３０１と第２ノード３０２との間でデータを送信するためのデ

ータリンクは、様々なタイプの接続媒体、例えば、有線リンク、無線リンク（例えばＷｉ－Ｆｉ（登録商標）またはＢｌｕｅｔｏｏｔｈ）または光ファイバリンクを含み得る。

【０１８６】

任意選択で、第１ノード３０１は、通信を開始する側であり得、マスターノードと称され得る。それに対応して、第２ノード３０２は、通信の受信側であり、セカンダリノードと称され得る。

【０１８７】

ノードにおける暗号化された内容が公開されないことを確実にするべく、鍵の使用期間は通常、限定されている。したがって、鍵更新の仕組みを導入する必要がある。例えば、Ｂｌｕｅｔｏｏｔｈを通じて接続されるＣＤＣ４０１およびカメラ４０２を例とすると、Ｅ０暗号化方式が使用される場合、ＣＤＣ４０１およびカメラ４０２は、2^{28}のＢｌｕｅｔｏｏｔｈティック（ｔｉｃｋｓ）（約２３．３時間）内に鍵を１回更新する必要がある。高度暗号化標準（ａｄｖａｎｃｅｄ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ，ＡＥＳ）暗号化アルゴリズムが使用される場合、ＣＤＣ４０１およびカメラ４０２は、2^{38}ティック（約２．７２年）内に鍵を１回更新する必要がある。別の例として、マスター鍵およびセッション鍵を含むノードにおいて、マスター鍵およびカウンタ値を使用することによってセッション鍵が生成されるとき、カウンタ値が反転される（または、カウントの新ラウンドが再開する）前に、マスター鍵が更新される必要がある。鍵更新プロセスにおいて、鍵更新に使用され、ノード間で送信されるメッセージは、中間者攻撃に対して脆弱であり、これにより、データセキュリティに影響が生じる。この問題を解決するべく、本願の実施形態は、以下の方法を提供する。

【０１８８】

図５は、本願の実施形態による鍵更新方法の概略フローチャートである。鍵更新方法は、図３に示されるアーキテクチャに基づいて実装され得る。当該方法は、以下のステップを備えるが、それらに限定されない。

【０１８９】

ステップ：Ｓ５０１：第１ノードが第１鍵更新要求を第２ノードへ送信する。

【０１９０】

具体的には、第１鍵更新要求は、第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む。第１鍵ネゴシエーションパラメータは、第１目標鍵を生成するのに使用される鍵パラメータである。複数の任意選択のケースが以下のように説明される。

【０１９１】

ケース１：第１鍵ネゴシエーションパラメータが鍵ネゴシエーションアルゴリズムのパラメータＫＥｍを含み得る。説明を容易にするべく、鍵ネゴシエーションアルゴリズムのパラメータＫＥｍは第１鍵ネゴシエーションアルゴリズムパラメータと称され得る。

【０１９２】

鍵ネゴシエーションアルゴリズムがＤＨアルゴリズムである例において、第１ノードにおいて決定されるＤＨアルゴリズムのパラメータは、素数ｐ、乱数ｇ、乱数ａおよび計算値Ａを含む。計算値Ａは、以下の式、すなわち、$A = g^a \bmod p$を満たし、素数ｐおよび乱数ｇは更に、ＤＨアルゴリズムの別のパラメータを生成するために第２ノードによって使用される。任意選択で、素数ｐ、乱数ｇ、および計算値Ａが第２ノードへ送信される必要があるので、素数ｐ、乱数ｇおよび計算値Ａは、第１ノードの公開鍵とみなされ得る。それに対応して、乱数ａは第２ノードへ送信されないので、乱数ａは、第１ノードの秘密鍵とみなされ得る。任意選択で、第１ノードは、計算値Ａを第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍとして使用し、第１鍵更新要求を送信する前に素数ｐおよび乱数ｇを第２ノードへ送信するか、または、素数ｐ、乱数ｇ、および計算値Ａを第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍとして使用し、第１鍵更新要求を使用することによって、第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍを第２ノードへ送信し得る。

【０１９３】
ケース２：第１鍵ネゴシエーションパラメータは新規パラメータ（ｆｒｅｓｈ　ｐａｒａｍｅｔｅｒ）を含み得る。
【０１９４】
本願の本実施形態において、第１鍵更新要求における第１アイデンティティ認証情報は、第１ノードと第２ノードとの間の共有鍵を使用することによって生成され得る。説明を容易にするべく、第１鍵更新要求を生成するための共有鍵は、第１共有鍵と称され、第１共有鍵は、マスター鍵または事前共有鍵ＰＳＫなどの鍵であり得る。
【０１９５】
任意選択の解決策において、第１アイデンティティ認証情報は、暗号アルゴリズムを使用することによって生成され得る。暗号アルゴリズムがＨＭＡＣである例において、ＨＭＡＣは、１または複数の文字パラメータの入力を受信し、識別子を出力するために使用され、識別子は、第１アイデンティティ認証情報として使用され得る。以下では、ハッシュ関数がＨＭＡＣである例を説明のために使用する。
【０１９６】
例１：第１ノードによって生成された第１アイデンティティ認証情報ＡＵＴＨｍは、ＨＭＡＣ（ＰＳＫ）であり得、または言い換えれば、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ）である。
【０１９７】
例２：第１鍵ネゴシエーションパラメータがＳ１として示される場合、第１ノードによって生成される第１アイデンティティ認証情報ＡＵＴＨｍは、ＨＭＡＣ（ＰＳＫ、Ｓ１）であり得、または言い換えれば、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、Ｓ１）である。Ｓ１は上述のケース１における第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍであり得るか、または、上述のケース２における新規パラメータ（例えば、カウンタ値、シリアル番号、ランダム値、およびフレーム番号のうち少なくとも１つ）であり得る。
【０１９８】
例３：第１鍵更新要求が乱数値（１回使用される番号、ＮＯＮＣＥ）を更に含む場合、第１ノードによって生成された第１アイデンティティ認証情報ＡＵＴＨｍは、ＨＭＡＣ（ＰＳＫ、Ｓ１、ＮＯＮＣＥｍ）であり得（ＮＯＮＣＥｍは、第１ノードによって生成された乱数値である）、または言い換えれば、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、Ｓ１、ＮＯＮＣＥｍ）である。
【０１９９】
本願の本実施形態において、第１鍵更新要求は更に、第１目標鍵の有効期間（ｅｘｐｉｒａｔｉｏｎ）および第１更新時点についての少なくとも１つの情報を示し得る。第１更新時点は、第１目標鍵が有効化される時間を示すために使用され、有効化時間または開始時点とも称され得る。
【０２００】
例えば、第１鍵更新要求は、第１目標鍵の有効期間を示す第１インジケーション情報を含む。第１インジケーション情報は、特定の日時であり得る。例えば、第１インジケーション情報が２０２０年２月６日の００：５２：５０である場合、第１目標鍵の有効日時が２０２０年２月６日の００：５２：５０に終了すること、または、無効日時が２０２０年２月６日の００：５２：５０の後に開始することを示し得る。第１インジケーション情報は代替的に、有効時間または無効時間を示す文字列、例えば、２０２０年２月６日の００：５２：５０を示すタイムスタンプ「１５９０９２１５７０」であり得る。第１インジケーション情報は代替的に、タイマまたは同様のものであり得る。例えば、第１目標鍵の有効期間が１０００秒である場合、第１目標鍵は、生成または有効化された１０００秒後まで有効であることを示す。第２インジケーション情報は更に、フレーム番号などを含み得る。
【０２０１】
別の例として、第１鍵更新要求は、第１更新時点を示す第２インジケーション情報を含

む。第２インジケーション情報は、フレーム番号、特定の日時、文字列、タイマ、または同様のもの１または複数であり得る。フレーム番号は、通信フレームの番号またはインデックスであり、通信フレームは、第１ノードが第２ノードと通信するときのメッセージ構造である。通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む。通信フレームのフレーム番号は通常、事前設定されたフレーム番号値範囲内で循環する。例えば、時分割多元接続ＴＤＭＡ通信技術において、時間は周期的フレームにセグメント化され、各フレームのフレーム番号は、０から２７１５６４７まで周期的に変化する。第１ノードは、更新要求において保持されるフレーム番号を使用することによって第１更新時点を示し得る。説明を容易にするべく、第１鍵更新要求において保持されるフレーム番号は、第１フレーム番号と称される。例えば、第１フレーム番号が２３４５である場合、フレーム番号２３４５から開始する通信フレームの後に第１目標鍵が適用されることを示す。任意選択で、第１フレーム番号は、複数のフレーム番号であり得る。例えば、第１フレーム番号が、ユーザプレーンダウンリンクフレームのフレーム番号Ａ、および、ユーザプレーンアップリンクフレームのフレーム番号Ｂを含み得る場合、第１目標鍵が、フレーム番号Ａから開始してそれに続くユーザプレーンダウンリンクフレームに適用されること、および、第１目標鍵が、フレーム番号Ｂから開始しそれに続くユーザプレーンアップリンクフレームに適用されることを示し得る。

【０２０２】

任意選択で、第１鍵更新要求が、第１フレーム番号を使用することによって第１更新時点を示す場合、第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示され得る。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ｍｅｄｉａ ａｃｃｅｓｓ ｃｏｎｔｒｏｌ ｓｅｒｉａｌ ｎｕｍｂｅｒ，ＭＡＣ ＳＮ）を含み、ＭＡＣ ＳＮは、Ｍビットを使用することによって示され、Ｍビットは、Ｆビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。説明を容易にするべく、第１フレーム番号が、本明細書における説明のために例として使用されるが、本発明を限定する意図は無い。

【０２０３】

第１鍵更新要求が有効期間および／または第１更新時点を更に含む場合、第１アイデンティティ認証情報について以下の例も存在し得る。

【０２０４】

例４：第１鍵更新要求が、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎを含む場合、第１ノードによって生成されたアイデンティティ認証情報ＡＵＴＨｍは、ＨＭＡＣ（ＰＳＫ、Ｓ１、ｅｘｐｉｒａｔｉｏｎ）であり得、または言い換えれば、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、Ｓ１、ｅｘｐｉｒａｔｉｏｎ）である。

【０２０５】

例５：第１鍵更新要求が、第１更新時点を示す情報ｔｉｍｅｒを含む場合、第１ノードによって生成されたアイデンティティ認証情報ＡＵＴＨｍは、ＨＭＡＣ（ＰＳＫ、Ｓ１、ｔｉｍｅｒ）であり得、または言い換えれば、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、Ｓ１、ｔｉｍｅｒ）である。有効化時間タイマは、新しい鍵が開始される時間を示す。

【０２０６】

例６：第１鍵更新要求が、乱数値ＮＯＮＣＥｍ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎ、および、第１更新時点を示す情報ｔｉｍｅｒを含む場合、第１ノードによって生成されたアイデンティティ認証情報ＡＵＴＨｍは、ＨＭＡＣ（ＰＳＫ、Ｓ１、

ＮＯＮＣＥｍ、ｅｘｐｉｒａｔｉｏｎ、ｔｉｍｅｒ）であり得、または言い換えれば、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、Ｓ１、ＮＯＮＣＥｍ、ｅｘｐｉｒａｔｉｏｎ、ｔｉｍｅｒ）である。

【０２０７】

当然、第１アイデンティティ認証情報が生成されるとき、第１共有鍵に加えて、他の情報（例えば、第１ノードの番号、第１ノードのアドレス、または、第１ノードと第２ノードとの間の接続の識別子）が含まれ得る。第１鍵更新要求が、乱数値ＮＯＮＣＥｍ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎ、および、第１更新時点を示す情報ｔｉｍｅｒなどのパラメータを含む場合、第１ノードは代替的に、第１世代アイデンティティ認証情報ＡＵＴＨｍにおけるパラメータの一部または全部を使用しないことがあり得ることに留意されたい。

【０２０８】

任意選択で、第１ノードは、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信し得、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用される。第１鍵更新要求において保持される第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。例えば、第３フレーム番号が２３６５である場合、フレーム番号が２３６５から開始する通信フレームの後に、前回更新された鍵が適用されること、および、第１ノードは、フレーム番号が２３６５に到達する前に、第１目標鍵を改めて決定する必要があることを示す。したがって、第１ノードは、フレーム番号が２３４５である第１通信フレームにおいて第１鍵更新要求を送信し得、第１フレーム番号２３５５は、第１鍵更新要求において第１目標鍵の開始時点を示すために使用される。通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行するためのものであり得る。したがって、フレーム番号が、前回更新された鍵のフレーム番号まで繰り返す前に、第１目標鍵が決定され、その結果、第１目標鍵を使用することによってデータフレームが暗号化される。このように、同一のフレーム番号を有するデータフレームは、異なる鍵を使用することによって２回暗号化でき、これにより、データセキュリティを改善する。

【０２０９】

代替的解決策において、第１鍵更新要求は、第１フレーム番号の代わりにＭＡＣシリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮはＭビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。代替的に、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号はまた、ＭＡＣ　ＳＮ、すなわち、第３フレーム番号を示すために使用される複数のビットの一部によって示されるＭＡＣ　ＳＮで置き換えられ得る。この代替的解決策において、第１フレーム番号、第２フレーム番号、および第３フレーム番号の間の値関係は変化しないままである。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０２１０】

任意選択で、第１目標鍵および前回更新された鍵は、同一タイプの鍵である。例えば、第１鍵更新要求において更新を要求された第１目標鍵が暗号化鍵であるとき、第３フレーム番号は、前回暗号化鍵を更新するために使用された鍵更新要求において保持されるフレーム番号である。

【０２１１】

任意選択で、第１ノードは、通信フレームのフレーム番号を記録し、通信フレームのフ

レーム番号および第３フレーム番号が第１閾値以下であるときに第１鍵更新要求を送信し得る。例えば、第１ノードは、第１閾値を２０に事前設定する。第３フレーム番号が２３６５である場合、第１ノードは、フレーム番号が２３４５である通信フレームを記録するとき、第１鍵更新要求を送信し得る。更に、第１ノードは、１または複数の通信フレームのフレーム番号を記録し得、例えば、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、または、ユーザプレーンダウンリンクフレームのうち少なくとも２つのフレーム番号を記録し得る。１つの通信フレームのフレーム番号と第３フレーム番号との間の相違点が第１閾値に到達した場合、第１鍵更新要求が送信される。

【０２１２】

任意選択で、前回の鍵更新のプロセスにおいて、鍵開始時点を示す情報が保持されないか、または、第１ノードが以前に鍵更新を実行していない場合、第１ノードは目標フレーム番号を事前構成し得る。現在の通信フレーム番号と目標フレーム番号との間の相違点が第１閾値以下であると第１ノードが検出した場合、第１ノードは第１鍵更新要求を送信する。前回の鍵更新において保持される第３フレーム番号を取得することに加えて、第１ノードは、前回の鍵更新中に送信された鍵更新要求におけるフレーム番号、応答メッセージが前回受信されたときのフレーム番号、または、前回更新された鍵が通信に初めて使用されたときに使用された通信フレームのフレーム番号を記録し、現在の鍵が更新される必要があるかどうかを検出し得ることに留意されたい。

【０２１３】

ステップＳ５０２：第２ノードが第１共有鍵に基づいて第１アイデンティティ認証情報に対して検証を実行する。

【０２１４】

具体的には、第１アイデンティティ認証情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第１ノードによって生成される。したがって、第２ノードは、第１共有鍵に基づいて、第１アイデンティティ認証情報が正確かどうかを検証し得る。

【０２１５】

任意選択の解決策において、プロトコルは、第１ノードが特定のパラメータを使用して第１アイデンティティ認証情報を生成すること、したがって、第２ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第１アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。例えば、第１アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成される。したがって、第２ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第１アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。

【０２１６】

例えば、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫに基づくＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証が成功する。

【０２１７】

別の例として、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ、Ｓ１）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫおよび第１鍵ネゴシエーションパラメータＳ１に基づいてＨＭＡＣを使用することによってチェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ、Ｓ１）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証が成功する。第１鍵ネゴシエーションパラメータＳ１については、ステップＳ５０１における対応する説明を参照されたい。

【０２１８】

任意選択で、第１アイデンティティ情報上の検証が失敗した場合、第１ノードのアイデンティティが信用できないことを示す。したがって、第２ノードは、その後の鍵更新ステップを実行しないことがあり得る。この場合、第２ノードは、第１ノードとの通信接続を切断し得るか、または、第２ノードは、更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは、第１鍵更新要求を破棄して応答せず、これにより、第２ノードのデータセキュリティを確実にする。

【０２１９】

任意選択で、第２ノードは、第１鍵更新要求のメッセージ完全性に対する検証を実行し、第１鍵更新要求における情報が別のデバイスによって改ざんされることを防止し得る。第１鍵更新要求は完全性保護検証識別子を含み得る。第２ノードは、完全性保護検証識別子を使用することによって、第１鍵更新要求のメッセージ完全性に対する検証を実行する。検証が成功した場合、第２ノードは続いて、第１アイデンティティ認証情報に対して検証を実行するステップを実行する。検証が失敗した場合、第２ノードは、第１ノードとの通信接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得るか、または、第２ノードは、第１鍵更新要求を破棄して応答せず、これにより、第２ノードのデータセキュリティを確実にする。

【０２２０】

ステップＳ５０３：第１アイデンティティ認証情報に対する検証が成功した場合、第２ノードは、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する。

【０２２１】

具体的には、第２ノードは、少なくとも以下の４つの任意選択の方法を使用することによって、第１鍵更新要求における第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する。

【０２２２】

方法１：第１鍵ネゴシエーションパラメータが上述のケース１を満たし、すなわち、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍを含み、第２ノードは、鍵ネゴシエーションアルゴリズムの第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを決定し得る。第２ノードは、第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍおよび第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓに基づいて、第１目標鍵を生成し得る。

【０２２３】

鍵ネゴシエーションアルゴリズムがＤＨアルゴリズムである例において、第２ノードによって第１ノードから受信されるＤＨアルゴリズムのパラメータは、素数ｐ、乱数ｇ、および第１計算値Ａを含み得、第２ノードによって決定され得る、ＤＨアルゴリズムのパラメータは、乱数ｂおよび計算値Ｂ、すなわち、第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを含み、ここで、Ｂは以下の式、$B = g^b \mod p$を満たす。第２ノードは、乱数ｂ、計算値Ａ、および素数ｐに基づいて、第１目標鍵Ｋ１を決定し得、Ｋ１は以下の式、$K1 = A^b \mod p$を満たす。

【０２２４】

任意選択で、第２ノードによって決定されるＤＨアルゴリズムのパラメータにおいて、乱数ｂは、第１目標鍵を生成するために第２ノードによって使用され、したがって、乱数ｂは第２ノードの秘密鍵とみなされ得、計算値Ｂは第１ノードへ送信され、したがって、計算値Ｂは第２ノードの公開鍵とみなされ得る。

【０２２５】

方法２：第１鍵ネゴシエーションパラメータは、上述のケース２を満たし、すなわち、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第２ノードは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成し得る。第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得る。

【０２２６】

任意選択で、第２ノードは、ＫＤＦを使用することによって第１目標鍵を生成し得る。

【０２２７】
例えば、第２ノードは、第２目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいてＫＤＦアルゴリズムを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ）であると決定する。
【０２２８】
方法３：第１鍵ネゴシエーションパラメータが上述のケース２を満たし、すなわち、第１鍵ネゴシエーションパラメータは新規パラメータを含む。アルゴリズム識別子ｔａｇが第２ノードから取得される場合、第２ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、およびアルゴリズム識別子ｔａｇに基づいて、ＫＤＦアルゴリズムを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ）であると決定し得る。
【０２２９】
アルゴリズム識別子は、第１目標鍵を生成するために使用されるアルゴリズムを示すために使用され得る。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成するために使用されるアルゴリズムを示すために使用される。別の例として、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成するために使用されるアルゴリズムを示すために使用される。アルゴリズム識別子は代替的に、使用されるハッシュアルゴリズムの識別子を示すために使用され得る。例えば、文字列「ＳＨＡ２５６」は、第１目標鍵がＳＨＡ２５６アルゴリズムであると決定するために使用されるアルゴリズムを示すために使用される。アルゴリズム識別子は代替的に、数値を使用することによって表され得る。例えば、０１はＡＥＳ暗号化アルゴリズムを表し、１０はメッセージ認証に基づくＡＥＳアルゴリズム（ＡＥＳ－ｃｙｐｈｅｒ－ｂａｓｅｄ ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ，ＡＥＳ－ＣＭＡＣ）完全性アルゴリズムを表す。
【０２３０】
アルゴリズム識別子は、第１ノードと第２ノードとの間で事前設定され得るか、または、第１ノードによって決定された後に第２ノードへ送信され得る。
【０２３１】
方法４：第１鍵ネゴシエーションパラメータが上述のケース２を満たし、すなわち、第１鍵ネゴシエーションパラメータは新規パラメータを含む。アルゴリズム識別子ｔａｇおよびアルゴリズムタイプｔｙｐｅが第２ノードから取得される場合、第２ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、アルゴリズム識別子ｔａｇ、および鍵タイプｔｙｐｅに基づいて、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ、ｔｙｐｅ）であると決定し得、ｔｙｐｅは鍵タイプを表す。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成することを示すために使用される。別の例として、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成することを示すために使用される。アルゴリズム識別子は、第１目標鍵を生成するために使用されるアルゴリズムを示すために使用される。
【０２３２】
鍵タイプは第１鍵更新要求において示され得るか、または、第１目標鍵が生成される前に第１ノードおよび第２ノードによって事前ネゴシエーションされ得る。
【０２３３】
任意選択で、方法２、方法３および方法４の任意の１または複数における第１目標鍵を決定するプロセスにおいて、第２ノードはまず、第１目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて中間鍵を決定し、次に、中間鍵に基づいて、アルゴリズム識別子ｔａｇおよび鍵タイプｔｙｐｅの少なくとも１つを使用することによって第１目標鍵Ｋ１を決定し得る。例えば、第２ノードは、鍵導出関数ＫＤＦ１を使用することによって中間鍵Ｋｍｉｄ：Ｋｍｉｄ＝ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）を取得し、次に、中間鍵Ｋｍｉｄに基づいて、鍵導出関数ＫＤＦ２を使用することによって、第１目標鍵Ｋ１：Ｋ１＝ＫＤＦ２（Ｋｍｉｄ、ｔａｇ、ｔｙｐｅ）を決定する。ＫＤＦ１およびＫＤＦ２は同一の鍵導出関数であり得るか、または、異なる鍵導出関数であり得る。この場合、第１ノードは、中間

鍵Ｋｍｉｄを決定するとき、新しい新規パラメータを生成するだけでよく、第１目標が決定されるたびに新しい新規パラメータを生成する必要がなく、これにより、新規パラメータを生成する回数の量を低減し、生成された新規パラメータの管理を容易にする。本明細書において本解決策をより明確に説明するために、第１目標鍵をどのように取得するかは、２つのステップを使用することによって説明されることに留意されたい。実際の処理において、第１目標鍵は代替的に、１つのステップを使用することによって取得され得る。中間鍵Ｋｍｉｄは中間結果に過ぎない。言い換えれば、第１目標を決定する方式は、Ｋ１＝ＫＤＦ２（ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）、ｔａｇ、ｔｙｐｅ）を満たす。

【０２３４】

任意選択で、第１鍵更新要求が第１更新時点を示す情報を保持するとき、第２ノードにおいて生成された第１目標鍵は、第１更新時点から開始する時間の後に適用される。任意選択で、第１フレーム番号を使用することによって第１更新時点が示されるとき、第１目標鍵は、第１更新時点から開始する通信フレームの後に適用される。

【０２３５】

任意選択で、第２ノードは、前回の鍵更新中に使用された鍵更新要求に保持される第３フレーム番号（または第３フレーム番号に対応するＭＡＣシリアル番号）を取得し得る。通信フレームのフレーム番号が１回反転された（またはカウントの新ラウンドが再開した）ことを第２ノードが検出した場合、現在の通信フレームのフレーム番号は、第３フレーム番号（または、第３フレーム番号に対応するＭＡＣシリアル番号）以上であり、この時点ではいかなる鍵更新要求も受信されず、または、いかなる新しい鍵も適用されず、第２ノードは第１ノードへの接続を切断し得、更にセキュリティコンテキストを削除して、他方への接続を再開し得、これにより、通信プロセスにおけるセキュリティを確実にする。セキュリティコンテキストは、共有鍵、鍵有効期間、および鍵更新時点などの少なくとも１つのセキュリティ情報を含む。

【０２３６】

任意選択で、第２ノードは更に、前回更新された鍵が初めて通信に使用されるときに使用される通信フレームのフレーム番号を取得し得る。通信フレームのフレーム番号が１回反転されたことを第２ノードが検出した場合、現在の通信フレームのフレーム番号は、前回更新された鍵が初めて通信に使用されたときに使用された通信フレームのフレーム番号以上であり、この時点では、いかなる鍵更新要求も受信されず、または、いかなる新しい鍵も適用されず、第２ノードは、第１ノードへの接続を切断し得、更にセキュリティコンテキストを削除し得、これにより、通信プロセスにおけるセキュリティを確実にする。

【０２３７】

ステップＳ５０４：第２ノードが第１応答メッセージを第１ノードへ送信する。

【０２３８】

具体的には、第１応答メッセージは、第２ノードのアイデンティティに対する認証を実行するために使用される第２アイデンティティ認証情報を含む。第２ノードが方法１を使用することによって第１目標鍵を生成する場合、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを含む。任意選択で、第１応答メッセージは更に、第２ノードによって生成された乱数値ＮＯＮＣＥｓを含む。

【０２３９】

本願の本実施形態において、第２アイデンティティ認証情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第２ノードによって生成され得る。

【０２４０】

任意選択の解決策において、第２アイデンティティ認証情報は、暗号アルゴリズムを使用することによって生成され得る。暗号アルゴリズムがＨＭＡＣである例において、ＨＭＡＣは、１または複数の文字パラメータの入力を受信し、識別子を出力するために使用され、識別子はアイデンティティ認証情報として使用され得る。以下では、暗号アルゴリズムがＨＭＡＣである例を説明のために使用する。

【０２４１】

例１：第２ノードによって生成された第２アイデンティティ認証情報ＡＵＴＨｓは、ＨＭＡＣ（ＰＳＫ）であり得、または言い換えれば、ＡＵＴＨｓ＝ＨＭＡＣ（ＰＳＫ）である。

【０２４２】

例２：第１応答メッセージが第２鍵ネゴシエーションパラメータＫＥｓを更に含むとき、第２ノードによって生成された第２アイデンティティ認証情報ＡＵＴＨｓは、ＨＭＡＣ（ＰＳＫ、ＫＥｓ）であり得、または言い換えれば、ＡＵＴＨｓ＝ＨＭＡＣ（ＰＳＫ、ＫＥｓ）である。

【０２４３】

例３：第１応答メッセージが、第２ノードによって生成された乱数値ＮＯＮＣＥｓを更に含むとき、第２ノードによって生成されたアイデンティティ認証情報ＡＵＴＨｓは、ＨＭＡＣ（ＰＳＫ、ＫＥｓ、ＮＯＮＣＥｓ）であり、または言い換えれば、ＡＵＴＨｓ＝ＨＭＡＣ（ＰＳＫ、Ｋ１、ＮＯＮＣＥｓ）であり得る。

【０２４４】

当然、第２アイデンティティ認証情報を生成するために使用されるパラメータにおいて、第１共有鍵に加えて、他の情報（例えば、第２ノードの番号、第２ノードのアドレス、または、第２ノードと第１ノードとの間の接続の識別子）が含まれ得る。第１応答メッセージが第２鍵ネゴシエーションパラメータＫＥｓおよび／または乱数値ＮＯＮＣＥｓなどのパラメータを含む場合、第２ノードは、これらのパラメータを使用してアイデンティティ認証情報ＡＵＴＨｓを生成しないことがあり得る。

【０２４５】

任意選択で、第１応答メッセージは、第２ノードが第１鍵ネゴシエーションパラメータおよび第１共有鍵に基づいて第１アイデンティティ認証情報を認証できる後に送信される応答メッセージである。

【０２４６】

ステップＳ５０５：第１ノードが第１共有鍵を使用することによって第２アイデンティティ認証情報に対して検証を実行する。

【０２４７】

具体的には、第２アイデンティティ情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第２ノードによって生成される。したがって、第１ノードは、第１共有鍵に基づいて、第２アイデンティティ認証情報が正確かどうかを検証し得る。

【０２４８】

任意選択の解決策において、プロトコルは、第２ノードが特定のパラメータを使用して第２アイデンティティ認証情報を生成すること、したがって、第１ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第２アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。

【０２４９】

例えば、第２アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成され得る。したがって、第１ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第２アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。

【０２５０】

例えば、第２アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。

【０２５１】

別の例として、第１アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ、ＫＥｓ

）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫ、ならびに、第１応答メッセージにおける第２鍵ネゴシエーションパラメータＫＥｓに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ、ＫＥｓ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。

【０２５２】

任意選択で、第２アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことが示される。したがって、第１ノードは、第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄して応答しないことがあり得、これにより、データ更新プロセスにおけるデータセキュリティを確実にし、鍵更新を実行する必要があるノードへの接続を容易にする。

【０２５３】

任意選択で、第１ノードは、第１応答メッセージのメッセージ完全性に対する検証を実行し、第１応答メッセージにおける情報が別のデバイスによって改ざんされることを防止し得る。第２ノードは完全性保護検証識別子を第１応答メッセージに追加し得る。第１ノードは、完全性保護検証識別子を使用することによって、第１応答メッセージのメッセージ完全性に対して検証を実行する。検証が成功した場合、第１ノードは続いて、第２アイデンティティ認証情報に対して検証を実行するステップを実行する。検証が失敗した場合、第１ノードは、第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄して応答しないことがあり得、これにより、データ更新プロセスにおけるデータセキュリティを確実にする。

【０２５４】

ステップＳ５０６：第２アイデンティティ認証情報に対する検証が成功した場合、第１ノードは、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する。

【０２５５】

具体的には、第１ノードは、少なくとも以下の複数の任意選択の方法を使用することによって、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する。

【０２５６】

方法１：第１鍵ネゴシエーションパラメータが上述のケース１を満たし、すなわち、第１鍵ネゴシエーションパラメータが鍵ネゴシエーションアルゴリズムのパラメータを含み、第１応答メッセージが第２鍵ネゴシエーションパラメータＫＥｓを含む。第１ノードは、第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍおよび第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓに基づいて第１目標鍵を生成し得る。

【０２５７】

鍵ネゴシエーションアルゴリズムがＤＨアルゴリズムである例において、第１ノードにおいて生成されるＤＨアルゴリズムのパラメータは、素数ｐ、乱数ｇ、乱数ａ、および第１計算値Ａを含む。第１ノードによって第２ノードから受信されるＤＨアルゴリズムのパラメータは第１計算値Ｂを含む。第１ノードは、乱数ａ、計算値Ｂおよび素数ｐに基づいて第１目標鍵Ｋ１を決定し得、Ｋ１は以下の式、すなわち、$K1 = B^a \bmod p$を満たす。$K1 = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a = B^a \bmod p$であるので、第１ノードおよび第２ノードによって決定される第１目標鍵Ｋ１は同一である。

【０２５８】

方法２：第１鍵ネゴシエーションパラメータが上述のケース２を満たし、すなわち、第１鍵ネゴシエーションパラメータが新規パラメータを含み、第１ノードは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成する。

【０２５９】

任意選択で、第１ノードはＫＤＦを使用することによって第１目標鍵を生成し得る。

【０２６０】
例えば、第１ノードは、第２目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて、ＫＤＦを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ）であると決定する。
【０２６１】
方法３：第１鍵ネゴシエーションパラメータが上述のケース２を満たし、すなわち、第１鍵ネゴシエーションパラメータは新規パラメータを含む。アルゴリズム識別子ｔａｇが第１ノードから取得される場合、第１ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、およびアルゴリズム識別子ｔａｇに基づいて、ＫＤＦアルゴリズムを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ）であると決定し得る。
【０２６２】
アルゴリズム識別子は、第１目標鍵を生成するために使用されるアルゴリズムを示すために使用され得る。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成するために使用されるアルゴリズムを示すために使用される。別の例として、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成するために使用されるアルゴリズムを示すために使用される。アルゴリズム識別子は代替的に、使用されるハッシュアルゴリズムの識別子を示すために使用され得る。例えば、文字列「ＳＨＡ２５６」は、第１目標鍵がＳＨＡ２５６アルゴリズムであると決定するために使用されるアルゴリズムを示すために使用される。アルゴリズム識別子は代替的に、数値を使用することによって表され得る。例えば、０１はＡＥＳ暗号化アルゴリズムを表し、１０はメッセージ認証に基づくＡＥＳアルゴリズム（ＡＥＳ－ｃｙｐｈｅｒ－ｂａｓｅｄ ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ，ＡＥＳ－ＣＭＡＣ）完全性アルゴリズムを表す。
【０２６３】
アルゴリズム識別子は、第１ノードと第２ノードとの間で事前設定され得るか、または、第１ノードによって決定され得る。
【０２６４】
方法４：第１鍵ネゴシエーションパラメータが上述のケース２を満たし、すなわち、第１鍵ネゴシエーションパラメータは新規パラメータを含む。アルゴリズム識別子ｔａｇおよびアルゴリズムタイプｔｙｐｅが第１ノードから取得される場合、第１ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、アルゴリズム識別子ｔａｇ、および鍵タイプｔｙｐｅに基づいて、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ、ｔｙｐｅ）であると決定し得、ｔｙｐｅは鍵タイプを表す。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成することを示すために使用される。別の例として、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成することを示すために使用される。アルゴリズム識別子は、第１目標鍵を生成するために使用されるアルゴリズムを示すために使用される。
【０２６５】
鍵タイプは第１鍵更新要求において示され得るか、または、第１目標鍵が生成される前に第１ノードおよび第２ノードによって事前ネゴシエーションされ得る。
【０２６６】
任意選択で、方法２、方法３および方法４の任意の１または複数における第１目標鍵を決定するプロセスにおいて、第１ノードはまず、第１目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて中間鍵を決定し、次に、中間鍵に基づいて、アルゴリズム識別子ｔａｇおよび鍵タイプｔｙｐｅの少なくとも１つを使用することによって第１目標鍵Ｋ１を決定し得る。例えば、第１ノードは、鍵導出関数ＫＤＦ１を使用することによって中間鍵Ｋｍｉｄ：Ｋｍｉｄ＝ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）を取得し、次に、中間鍵Ｋｍｉｄに基づいて、鍵導出関数ＫＤＦ２を使用することによって、第１目標鍵Ｋ１＝ＫＤＦ２（Ｋｍｉｄ、ｔａｇ、ｔｙｐｅ）を決定する。ＫＤＦ１およびＫＤＦ２は同一の鍵導出関数であり得るか、または、異なる鍵導出関数であり得る。本明細書において本解決策をより明確

に説明するために、第１目標鍵をどのように取得するかは、２つのステップを使用することによって説明される。実際の処理において、第１目標鍵は代替的に、１つのステップを使用することによって取得され得る。中間鍵Ｋｍｉｄは中間結果に過ぎない。言い換えれば、第１目標を決定する方式は、Ｋ１＝ＫＤＦ２（ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）、ｔａｇ、ｔｙｐｅ）を満たす。

【０２６７】

任意選択で、第１目標鍵は、第１ノードと第２ノードとの間の共有鍵に適用され得、マスター鍵、セッション鍵などを含む。

【０２６８】

任意選択で、第１鍵更新要求が第１更新時点を示す場合、第１目標鍵は、第１更新時点から開始する時間内に適用され得る。例えば、第１目標鍵がマスター鍵であり、かつ、第１鍵更新要求に含まれる第１秘密鍵を示す情報がタイムスタンプ「１５９０９２１５７０」である場合、第１目標鍵が有効化される時間は２０２０年２月６日の００：５２：５０であること、したがって、第１ノードおよび第２ノードは、２０２０年２月６日の００：５２：５０に開始する時間の後に第１目標鍵をマスター鍵として使用することを示す。

【０２６９】

任意選択で、第１鍵更新要求が第１目標鍵の有効期間を示す場合、第１目標鍵は、第１目標鍵の有効期間内に適用され得る。例えば、第１目標鍵がマスター鍵であり、かつ、第１鍵更新要求に含まれる第１秘密鍵を示す情報がタイムスタンプ「１５９０９５２４４７」である場合、第１目標鍵の有効期間は２０２０年２月６日の０９：２８：２６であること、したがって、第１ノードおよび第２ノードは、２０２０年２月６日の０９：２８：２６に第１目標鍵をマスター鍵として使用し得ることを示す。

【０２７０】

任意選択で、第２ノードは更に、第１目標鍵の有効期間を検出して、第１目標鍵の有効期間の前に新しい目標鍵を決定し得る。

【０２７１】

第１鍵更新要求が第１更新時点および第１目標鍵の有効期間を示すとき、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用されることが理解され得る。

【０２７２】

任意選択で、第２目標鍵は暗号化鍵であり得る。この場合、第１鍵更新要求は第２目標鍵を使用することによって暗号化され得る。それに対応して、第２ノードは、第１鍵更新要求を受信した後に、解読のために第２目標鍵を使用し得る。同様に、第１応答要求は、第２目標鍵を使用することによって暗号化され得る。それに対応して、第１ノードは、第１応答メッセージを受信した後に、第２目標鍵を解読に使用し得る。

【０２７３】

任意選択で、第２目標鍵は完全性保護鍵であり得る。この場合、完全性保護は、第２目標鍵を使用することによって第１鍵更新要求に対して実行され得る。それに対応して、第２ノードは、第１鍵更新要求を第１ノードから受信した後に、第２目標鍵を使用することによってデータ完全性をチェックし得る。同様に、完全性保護は、第２目標鍵を使用することによって第１応答要求に対して実行され得る。それに対応して、第１ノードは、第１応答メッセージを受信した後に、第２目標鍵を使用することによってデータ完全性をチェックし得る。従来の鍵更新プロセスにおいて、鍵更新時点が構成される。したがって、新しい鍵が更新されるとき、古い鍵が失効したので、暗号化プロセスは鍵更新中に保留される必要があり、暗号化プロセスは、鍵更新が完了した後に再開する。しかしながら、暗号化プロセスの保留および暗号化プロセスの再開は鍵更新効率に影響を与え、暗号化プロセスの保留はセキュリティに影響を与える。しかしながら、本願における鍵更新方法において、古い鍵が失効する前に鍵が更新される。古い鍵は失効していないので、暗号化プロセスは保留される必要が無く、これにより、鍵更新効率を改善し、データセキュリティを改善する。

【０２７４】

任意選択で、第２目標鍵はマスター鍵であり得る。この場合、第２目標鍵は、暗号化鍵または完全性保護鍵を決定するために使用され得る。したがって、暗号化および／または完全性保護は、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求に対して実行され得る。それに対応して、第２ノードは、第１鍵更新要求を受信した後に、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１鍵更新要求を解読し得、および／または、第２目標鍵に基づいて決定された完全性保護鍵は、第２目標鍵に基づいて決定された完全性保護鍵を使用することによってデータ完全性をチェックするために使用され得る。同様に、暗号化および／または完全性保護は、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１応答要求に対して実行され得る。それに対応して、第１ノードは、第１応答メッセージを受信した後に、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、第１応答メッセージを解読し得、および／または、第２目標鍵に基づいて決定された完全性保護鍵は、第２目標鍵に基づいて決定された完全性保護鍵を使用することよってデータ完全性をチェックするために使用され得る。

【０２７５】

任意選択で、方法２および方法３を使用することによって第１目標鍵が決定されたとき、第１目標鍵がセッション鍵である場合、暗号化または完全性保護が、第１目標鍵を使用することによって、第１応答メッセージに対して実行され得る。

【０２７６】

任意選択で、第１ノードがマスター鍵およびカウンタ値を使用することによってセッション鍵を更新するとき、第１ノードは、カウンタ値が反転された（または、カウントの新ラウンドが再開した）かどうかを検出し、カウンタ値が反転される前に第１鍵更新要求を第２ノードへ送信する（決定された第１目標鍵はマスター鍵である）。任意選択で、カウンタ値が反転される前に第１ノードが第１鍵更新要求を送信しない場合、第１ノードは、第２ノードへの通信接続を切断して第２ノードに再アクセスし得、これにより、第２ノードとの通信のプロセスのセキュリティを確実にする。

【０２７７】

任意選択で、第１ノードは、前回の鍵更新中に使用された鍵更新要求に保持される第３フレーム番号（または第３フレーム番号に対応するＭＡＣシリアル番号）を取得し得る。通信フレームのフレーム番号が１回反転されたことを第１ノードが検出した場合、現在の通信フレームのフレーム番号は、第３フレーム番号（または第３フレーム番号に対応するＭＡＣシリアル番号）以上であり、この時点では、いかなる鍵更新要求も送信されず、または、いかなる新しい鍵も適用されず、第１ノードは、第２ノードへの接続を切断し得、セキュリティコンテキストを更に削除し得、他方への接続を再開し、これにより、通信プロセスにおけるセキュリティを確実にする。

【０２７８】

図５に説明される方法では、鍵更新プロセスにおいて、第１ノードおよび第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第１鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０２７９】

図５に示される前述の方法の実施形態は、多くの可能な実装の解決策を含む。以下では、図６Ａ、図６Ｂ、図７Ａ、図７Ｂ、図８Ａ、および図８Ｂを参照して、いくつかの実装の解決策を別々に説明する。図６Ａ、図６Ｂ、図７Ａ、図７Ｂ、図８Ａおよび図８Ｂにお

いて説明されない関連する概念またはオペレーションまたは論理関係については、図５に示される実施形態における対応する説明が参照されることに留意されたい。したがって、詳細は再度説明されない。

【０２８０】

図６Ａおよび図６Ｂは、本願の実施形態によるなお別の鍵更新方法を示す。方法は少なくとも以下のステップを含む。

【０２８１】

ステップＳ６０１：第１ノードが第１鍵更新要求を第２ノードへ送信する。

【０２８２】

本願の本実施形態において、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性鍵を使用することによって、暗号化および／または完全性保護が第１鍵更新要求に対して実行され得る。第２目標鍵は、第１ノードと第２ノードとの間の共有鍵である。

【０２８３】

本願の本実施形態において、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む。第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍであり得る。任意選択で、第１鍵更新要求は更に、乱数値ＮＯＮＣＥｍ、第１更新時点を示す情報ｔｉｍｅｒ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎの少なくとも１つを含み得る。

【０２８４】

本願の本実施形態において、第１ノードと第２ノードとの間の第１共有鍵を使用することによって、第１鍵更新要求における第１アイデンティティ認証情報が生成され得、第１共有鍵は、マスター鍵、事前共有鍵ＰＳＫなどを含み得る。

【０２８５】

任意選択で、第１アイデンティティ認証情報を生成するための機能は暗号アルゴリズムであり得る。暗号アルゴリズムがＨＭＡＣであり第１共有鍵が事前共有鍵ＰＳＫである例において、生成された第１アイデンティティ認証情報ＡＵＴＨｍは、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、ＫＥｍ、ＮＯＮＣＥｍ、ｅｘｐｉｒａｔｉｏｎ、ｔｉｍｅｒ）として表され得、パラメータのシーケンスは異なり得る。当然、第１鍵更新要求が第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍ、乱数値ＮＯＮＣＥｍ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎ、または、第１更新時点を示す情報ｔｉｍｅｒなどのパラメータを含むとき、第１ノードは、第１アイデンティティ認証情報ＡＵＴＨｍを生成するためにパラメータの一部または全部を使用しないことがあり得る。

【０２８６】

任意選択で、第１ノードは、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信し得、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用される。第１鍵更新要求において保持される第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。例えば、第３フレーム番号が２３６５である場合、フレーム番号が２３６５から開始する通信フレームの後に、前回更新された鍵が適用されること、および、第１ノードは、フレーム番号が２３６５に到達する前に、第１目標鍵を改めて決定する必要があることを示す。したがって、第１ノードは、フレーム番号が２３４５である第１通信フレームにおいて第１鍵更新要求を送信し得、第１フレーム番号２３５５は、第１鍵更新要求において第１目標鍵の開始時点を示すために使用される。通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行するためのものであり得る。したがって、フレーム番号が、前回更新された鍵のフレーム番号まで繰り返す前に、第１目標鍵が決定され、その結果、第１目標鍵を使用することによってデータフレームが暗号化される。このように、同一のフレーム番号を有するデータフレームは、異なる鍵を使用すること

によって２回暗号化でき、これにより、データセキュリティを改善する。
【０２８７】
任意選択で、前回の鍵更新のプロセスにおいて、鍵開始時点を示す情報が保持されないか、または、第１ノードが以前に鍵更新を実行していない場合、第１ノードは目標フレーム番号を事前構成し得る。現在の通信フレーム番号と目標フレーム番号との間の相違点が第１閾値以下であると第１ノードが検出した場合、第１ノードは第１鍵更新要求を送信する。
【０２８８】
ステップＳ６０２：第２ノードが第１鍵更新要求を解読する。
【０２８９】
具体的には、第２ノードが、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１鍵更新要求を解読し得る。
【０２９０】
ステップＳ６０３：第２ノードが第１鍵更新要求のメッセージ完全性に対して検証を実行する。
【０２９１】
任意選択で、検証が失敗した場合、第２ノードは第１ノードへの通信接続を切断し得、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信し、または、第２ノードは第１鍵更新要求を破棄し得る。
【０２９２】
任意選択で、図６Ａおよび図６Ｂに示される実施形態において、第２ノードはステップＳ６０３を実行しないことがあり得る。この場合、第２ノードは、ステップＳ６０２を実行した後、続いてステップＳ６０４、および、ステップＳ６０４の後続のステップを実行し得る。
【０２９３】
ステップＳ６０４：第２ノードは第１アイデンティティ認証情報に対して検証を実行する。
【０２９４】
具体的には、第１アイデンティティ認証情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第１ノードによって生成される。したがって、第２ノードは、第１共有鍵に基づいて、第１アイデンティティ認証情報が正確かどうかを検証し得る。
【０２９５】
任意選択の解決策において、プロトコルは、第１ノードが特定のパラメータを使用して第１アイデンティティ認証情報を生成すること、したがって、第２ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第１アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。例えば、第１アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成される。したがって、第２ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１とも称される、検証に使用されるアイデンティティ認証情報を生成し得、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第１アイデンティティ認証情報が正確かどうかを検証する。以下では説明のために例を用いる。
【０２９６】
例えば、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫに基づくＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証が成功する。
【０２９７】
別の例として、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ、ＫＥｍ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫおよび

第１鍵ネゴシエーションパラメータＫＥｍに基づいてＨＭＡＣを使用することによってチェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ、ＫＥｍ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証が成功する。

【０２９８】

任意選択で、第１アイデンティティ情報に対する検証が失敗した場合、第２ノードは、第１ノードとの通信接続を切断し得るか、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは、第１鍵更新要求を破棄する。

【０２９９】

任意選択で、第２ノードはまず、Ｓ６０４のオペレーションを実行し、次に、Ｓ６０３のオペレーションを実行し得る。

【０３００】

ステップＳ６０５：第１アイデンティティ認証情報に対する検証が成功した場合、第２ノードは、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成する。

【０３０１】

具体的には、第２ノードは、鍵ネゴシエーションアルゴリズムの第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを決定し得る。第２ノードは、第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍおよび第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓに基づいて第１目標鍵を生成する。

【０３０２】

鍵ネゴシエーションアルゴリズムがＤＨアルゴリズムである例において、第２ノードによって第１ノードから受信されるＤＨアルゴリズムのパラメータは、素数ｐ、乱数ｇ、および第１計算値Ａを含み得、第２ノードによって決定され得る、ＤＨアルゴリズムのパラメータは、乱数ｂおよび計算値Ｂ、すなわち、第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを含み、ここで、Ｂは以下の式、$B = g^b \mod p$を満たす。第２ノードは、乱数ｂ、計算値Ａ、および素数ｐに基づいて、第１目標鍵Ｋ１を決定し得、Ｋ１は以下の式、$K1 = A^b \mod p$を満たす。

【０３０３】

ステップＳ６０６：第２ノードが第１応答メッセージを第１ノードへ送信する。

【０３０４】

本願の本実施形態において、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性鍵を使用することによって、暗号化および／または完全性保護が第１応答メッセージに対して実行され得る。第２目標鍵は第２ノードと第１ノードとの間の共有鍵である。

【０３０５】

第１応答メッセージは、第２アイデンティティ認証情報および第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを含み、第２アイデンティティ認証情報は、第２ノードのアイデンティティを検証するために使用され、第１ノードと第２ノードとの間の第１共有鍵を使用することによって生成され得る。任意選択で、第１応答メッセージは更に乱数値ＮＯＮＣＥｓを含み得る。

【０３０６】

本願の本実施形態において、第２アイデンティティ認証情報は、暗号アルゴリズムを使用することによって生成され得る。暗号アルゴリズムがＨＭＡＣである例において、生成された第２アイデンティティ認証情報ＡＵＴＨｓは、ＡＵＴＨｓ＝ＨＭＡＣ（ＰＳＫ、ＫＥｓ、ＮＯＮＣＥｓ）として表され得、パラメータのシーケンスは異なり得る。当然、第１鍵更新要求が第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓおよび乱数値ＮＯＮＣＥｓなどのパラメータを含むとき、第２ノードは、第２アイデンティティ認証情報ＡＵＴＨｓを生成するためにパラメータの一部または全部を使用しないことがあり得る。

【０３０７】

任意選択で、第２ノードはまず、Ｓ６０６のオペレーションを実行し、次に、Ｓ６０５

のオペレーションを実行し得る。
【０３０８】
ステップＳ６０７：第１ノードが第１応答メッセージを解読する。
【０３０９】
具体的には、第１ノードは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１応答メッセージを解読し得る。
【０３１０】
任意選択で、第１ノードはまず、Ｓ６０７のオペレーションを実行し、次にＳ６０６のオペレーションを実行し得る。
【０３１１】
ステップＳ６０８：第１ノードは第１応答メッセージのメッセージ完全性に対して検証を実行する。
【０３１２】
任意選択で、メッセージ完全性に対する検証が失敗した場合、第１ノードは第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄し得る。
【０３１３】
任意選択で、図６Ａおよび図６Ｂに示される実施形態において、第１ノードはステップＳ６０８を実行しないことがあり得る。この場合、ステップＳ６０７を実行した後に、第１ノードは続いてステップＳ６０９およびステップＳ６０９の後続のステップを実行し得る。
【０３１４】
ステップＳ６０９：第１ノードが第２アイデンティティ認証情報に対する検証を実行する。
【０３１５】
具体的には、第２アイデンティティ情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第２ノードによって生成される。したがって、第１ノードは、第１共有鍵に基づいて、第２アイデンティティ認証情報が正確かどうかを検証し得る。
【０３１６】
任意選択の解決策において、プロトコルは、第２ノードが特定のパラメータを使用して第２アイデンティティ認証情報を生成すること、したがって、第１ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第２アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。
【０３１７】
例えば、第２アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成され得る。したがって、第１ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第２アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。
【０３１８】
例えば、第２アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。
【０３１９】
別の例として、第１アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ、ＫＥｓ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫ、ならびに、第１応答メッセージにおける第２鍵ネゴシエーションパラメータＫＥｓに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ、ＫＥｓ

）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。

【０３２０】

任意選択で、第２アイデンティティ認証情報に対する検証が失敗した場合、第１ノードは、第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄し得る。

【０３２１】

任意選択で、第１ノードはまず、Ｓ６０９のオペレーションを実行し、次に、Ｓ６０８のオペレーションを実行し得る。

【０３２２】

ステップＳ６１０：第２アイデンティティ認証情報に対する検証が成功した場合、第１ノードは、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成する。

【０３２３】

具体的には、第１応答メッセージは第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓを含むので、第１ノードは、第１鍵ネゴシエーションアルゴリズムパラメータＫＥｍおよび第２鍵ネゴシエーションアルゴリズムパラメータＫＥｓに基づいて第１目標鍵を生成する。

【０３２４】

鍵ネゴシエーションアルゴリズムがＤＨアルゴリズムである例において、第１ノードにおいて生成されるＤＨアルゴリズムのパラメータは、素数ｐ、乱数ｇ、乱数ａ、および第１計算値Ａを含む。第１ノードによって第２ノードから受信されるＤＨアルゴリズムのパラメータは第１計算値Ｂを含む。第１ノードは、乱数ａ、計算値Ｂおよび素数ｐに基づいて第１目標鍵Ｋ１を決定し得、Ｋ１は以下の式、すなわち、$K1 = B^a \bmod p$を満たす。$K1 = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$であるので、第１ノードおよび第２ノードによって決定される第１目標鍵Ｋ１は同一である。

【０３２５】

任意選択で、第１目標鍵は、第１ノードと第２ノードとの間の共有鍵に適用され得るか、または、マスター鍵もしくはセッション鍵に適用され得る。

【０３２６】

図６Ａおよび図６Ｂにおいて説明される方法では、鍵更新プロセスにおいて、第１ノードおよび第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第１鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０３２７】

図７Ａおよび図７Ｂは、本願の実施形態による更に別の鍵更新方法を示す。方法は少なくとも以下のステップを含む。

【０３２８】

ステップＳ７０１：第１ノードが第１鍵更新要求を第２ノードへ送信する。

【０３２９】

本願の本実施形態において、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性鍵を使用することによって、暗号化および／または完全性保護が第１鍵更新要求に対して実行され得る。第２目標鍵は第２ノードと第１ノードとの間の共有鍵である。

【０３３０】

本願の本実施形態において、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む。第１鍵ネゴシエーションパラメータは新規パラメータｆｒｅｓｈであり得る。任意選択で、第１鍵要求は更に、乱数値ＮＯＮＣＥｍ、第１更新時点を示す情報ｔｉｍｅｒ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎの少なくとも１つを含み得る。

【０３３１】

本願の本実施形態において、第１ノードと第２ノードとの間の第１共有鍵を使用することによって、第１鍵更新要求における第１アイデンティティ認証情報が生成され得、第１共有鍵は、マスター鍵、事前共有鍵ＰＳＫなどを含み得る。

【０３３２】

任意選択で、第１アイデンティティ認証情報を生成するための機能は暗号アルゴリズムであり得る。暗号アルゴリズムがＨＭＡＣであり第１共有鍵が事前共有鍵ＰＳＫである例において、生成された第１アイデンティティ認証情報ＡＵＴＨｍは、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、ｆｒｅｓｈ、ＮＯＮＣＥｍ、ｅｘｐｉｒａｔｉｏｎ、ｔｉｍｅｒ）として表され得、パラメータのシーケンスは異なり得る。当然、第１鍵更新要求が新規パラメータｆｒｅｓｈ、乱数値ＮＯＮＣＥｍ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎ、または、第１更新時点を示す情報ｔｉｍｅｒなどの情報を含むとき、第１ノードは、第１アイデンティティ認証情報ＡＵＴＨｍを生成するためにパラメータの一部または全部を使用しないことがあり得る。

【０３３３】

任意選択で、第１ノードは、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信し得、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用される。第１鍵更新要求において保持される第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。例えば、第３フレーム番号が２３６５である場合、フレーム番号が２３６５から開始する通信フレームの後に、前回更新された鍵が適用されること、および、第１ノードは、フレーム番号が２３６５に到達する前に、第１目標鍵を改めて決定する必要があることを示す。したがって、第１ノードは、フレーム番号が２３４５である第１通信フレームにおいて第１鍵更新要求を送信し得、第１フレーム番号２３５５は、第１鍵更新要求において第１目標鍵の開始時点を示すために使用される。通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行するためのものであり得る。したがって、フレーム番号が、前回更新された鍵のフレーム番号まで繰り返す前に、第１目標鍵が決定され、その結果、第１目標鍵を使用することによってデータフレームが暗号化される。このように、同一のフレーム番号を有するデータフレームは、異なる鍵を使用することによって２回暗号化でき、これにより、データセキュリティを改善する。

【０３３４】

任意選択で、前回の鍵更新のプロセスにおいて、鍵開始時点を示す情報が保持されないか、または、第１ノードが以前に鍵更新を実行していない場合、第１ノードは目標フレーム番号を事前構成し得る。現在の通信フレーム番号と目標フレーム番号との間の相違点が第１閾値以下であると第１ノードが検出した場合、第１ノードは第１鍵更新要求を送信する。

【０３３５】

ステップＳ７０２：第２ノードが第１鍵更新要求を解読する。

【０３３６】

具体的には、第２ノードは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１鍵更新要求を解読し得る。

【０３３７】

ステップＳ７０３：第２ノードが第１鍵更新要求のメッセージ完全性に対する検証を実

行する。
【０３３８】
任意選択で、メッセージ完全性に対する検証が失敗した場合、第２ノードは、第１ノードへの通信接続を切断し得るか、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは第１鍵更新要求を破棄し得る。
【０３３９】
任意選択で、図７Ａおよび図７Ｂに示される実施形態において、第２ノードはステップＳ７０３を実行しないことがあり得る。この場合、ステップＳ７０２を実行した後に、第２ノードは続いて、ステップＳ７０４およびステップＳ７０４の後続のステップを実行し得る。
【０３４０】
ステップＳ７０４：第２ノードが第１アイデンティティ認証情報に対する検証を実行する。
【０３４１】
具体的には、第１アイデンティティ認証情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第１ノードによって生成される。したがって、第２ノードは、第１共有鍵に基づいて、第１アイデンティティ認証情報が正確かどうかを検証し得る。
【０３４２】
任意選択の解決策において、プロトコルは、第１ノードが特定のパラメータを使用して第１アイデンティティ認証情報を生成すること、したがって、第２ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第１アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。例えば、第１アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成される。したがって、第２ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第１アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。
【０３４３】
例えば、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫに基づくＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証は成功である。
【０３４４】
別の例として、第１鍵ネゴシエーションパラメータが新規パラメータｆｒｅｓｈを含み、かつ、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ、ｆｒｅｓｈ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫおよび新規パラメータｆｒｅｓｈに基づいて、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ、ｆｒｅｓｈ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証は成功である。
【０３４５】
任意選択で、第１アイデンティティ情報に対する検証が失敗した場合、第２ノードは、第１ノードとの通信接続を切断し得るか、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは、第１鍵更新要求を破棄する。
【０３４６】
任意選択で、具体的な実装プロセスにおいて、第２ノードはまず、Ｓ７０４のオペレーションを実行し、次に、Ｓ７０３のオペレーションを実行し得る。
【０３４７】
ステップＳ７０５：第１アイデンティティ認証情報に対する検証が成功した場合、第２ノードは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成する。

【０３４８】
任意選択で、第１アイデンティティ情報に対する検証が失敗した場合、第２ノードは、第１ノードとの通信接続を切断し得るか、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは、第１鍵更新要求を破棄する。
【０３４９】
具体的には、第２ノードは、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成し得る。例えば、第２ノードは、第２目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ）であると決定し得る。
【０３５０】
ステップＳ７０６：第２ノードが第１応答メッセージを第１ノードへ送信する。
【０３５１】
本願の本実施形態において、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性鍵を使用することによって、暗号化および／または完全性保護が第１鍵更新要求に対して実行され得る。第２目標鍵は第２ノードと第１ノードとの間の共有鍵である。
【０３５２】
第１応答メッセージは第２アイデンティティ認証情報を含み、第２アイデンティティ認証情報は、第２ノードのアイデンティティを検証するために使用され、第１ノードと第２ノードとの間の第１共有鍵を使用することによって生成され得る。任意選択で、第１応答メッセージは更に、乱数値ＮＯＮＣＥｓを含み得る。
【０３５３】
本願の本実施形態において、第２アイデンティティ認証情報を生成するためのアルゴリズムは暗号アルゴリズムであり得る。暗号アルゴリズムがＨＭＡＣである例において、生成された第２アイデンティティ認証情報ＡＵＴＨｓは、ＡＵＴＨｓ＝ＨＭＡＣ（ＰＳＫ、ＮＯＮＣＥｓ）として表され得、パラメータのシーケンスは異なり得る。当然、第１応答メッセージが乱数値ＮＯＮＣＥｓなどのパラメータを含むとき、第２ノードは、第２アイデンティティ認証情報ＡＵＴＨｓを生成するためにこれらのパラメータを使用しないことがあり得る。
【０３５４】
任意選択で、具体的な実装プロセスにおいて、第２ノードはまず、Ｓ７０６のオペレーションを実行し、次にＳ７０５のオペレーションを実行し得る。
【０３５５】
ステップＳ７０７：第１ノードが第１応答メッセージを解読する。
【０３５６】
具体的には、第１ノードは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１応答メッセージを解読し得る。
【０３５７】
ステップＳ７０８：第１ノードが第１応答メッセージのメッセージ完全性に対する検証を実行する。
【０３５８】
任意選択で、メッセージ完全性に対する検証が失敗した場合、第１ノードは第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄し得る。
【０３５９】
任意選択で、図７Ａおよび図７Ｂに示される実施形態において、第１ノードはステップＳ７０８を実行しないことがあり得る。この場合、ステップＳ７０７を実行した後に、第１ノードは続いて、ステップＳ７０９およびステップＳ７０９の後続のステップを実行し得る。
【０３６０】
ステップＳ７０９：第１ノードが第２アイデンティティ認証情報に対する検証を実行す

る。
【０３６１】
具体的には、第２アイデンティティ情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第２ノードによって生成される。したがって、第１ノードは、第１共有鍵に基づいて、第２アイデンティティ認証情報が正確かどうかを検証し得る。
【０３６２】
任意選択の解決策において、プロトコルは、第２ノードが特定のパラメータを使用して第２アイデンティティ認証情報を生成すること、したがって、第１ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第２アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。
【０３６３】
例えば、第２アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成され得る。したがって、第１ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第２アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。
【０３６４】
例えば、第２アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。
【０３６５】
別の例として、第１アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ、ＮＯＮＣＥｓ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫ、ならびに、第１応答メッセージにおける乱数値ＮＯＮＣＥｓに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ、ＮＯＮＣＥｓ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。
【０３６６】
任意選択で、第２アイデンティティ認証情報に対する検証が失敗した場合、第１ノードは、第２ノードへの通信接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄し得る。
【０３６７】
任意選択で、具体的な実装プロセスにおいて、第１ノードはまずＳ７０９のオペレーションを実行し、次に、Ｓ７０８のオペレーションを実行し得る。
【０３６８】
ステップＳ７１０：第２アイデンティティ認証情報に対する検証が成功した場合、第１ノードは第２目標鍵および新規パラメータに基づいて第１目標鍵を生成する。
【０３６９】
具体的には、第１ノードは、第２目標鍵および新規パラメータに基づいて鍵導出関数を使用することによって第１目標鍵を生成し得る。例えば、第２ノードは、第２目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ）であると決定し得る。
【０３７０】
任意選択で、第１目標鍵は、第１ノードと第２ノードとの間の共有鍵に適用され得、マスター鍵、セッション鍵などを含む。
【０３７１】
図７Ａおよび図７Ｂにおいて説明される方法では、鍵更新プロセスにおいて、第１ノードおよび第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、メッセージを他のノードから受信した後に、まずアイデンティティ認証情

報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第２目標鍵および新規パラメータに基づいて鍵を更新し、第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０３７２】

図８Ａおよび図８Ｂは、本願の実施形態による更に別の鍵更新方法を示す。当該方法は、以下のステップを備えるが、それらに限定されない。

【０３７３】

ステップＳ８０１：第１ノードが第１鍵更新要求を第２ノードへ送信する。

【０３７４】

本願の本実施形態において、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性鍵を使用することによって、暗号化および／または完全性保護が第１鍵更新要求に対して実行され得る。第２目標鍵は第２ノードと第１ノードとの間の共有鍵である。

【０３７５】

本願の本実施形態において、第１鍵更新要求は、第１鍵ネゴシエーションパラメータ、新規パラメータｆｒｅｓｈおよび第１アイデンティティ認証情報を含む。第１鍵ネゴシエーションパラメータは新規パラメータｆｒｅｓｈであり得る。任意選択で、第１鍵要求は更に、乱数値ＮＯＮＣＥｍ、第１更新時点を示す情報ｔｉｍｅｒ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎの少なくとも１つを含み得る。

【０３７６】

本願の本実施形態において、第１ノードと第２ノードとの間の第１共有鍵を使用することによって、第１鍵更新要求における第１アイデンティティ認証情報が生成され得、第１共有鍵は、マスター鍵、事前共有鍵ＰＳＫなどを含み得る。

【０３７７】

任意選択で、第１アイデンティティ認証情報を生成するためのアルゴリズムは暗号アルゴリズムであり得る。暗号アルゴリズムがＨＭＡＣである例において、生成された第１アイデンティティ認証情報ＡＵＴＨｍは、ＡＵＴＨｍ＝ＨＭＡＣ（ＰＳＫ、ｆｒｅｓｈ、ＮＯＮＣＥｍ、ｅｘｐｉｒａｔｉｏｎ、ｔｉｍｅｒ）として表され得、パラメータのシーケンスは異なり得る。当然、第１鍵更新要求が新規パラメータｆｒｅｓｈ、乱数値ＮＯＮＣＥｍ、第１目標鍵の有効期間を示す情報ｅｘｐｉｒａｔｉｏｎ、または、第１更新時点を示す情報ｔｉｍｅｒなどの情報を含むとき、第１ノードは、第１アイデンティティ認証情報ＡＵＴＨｍを生成するためにパラメータの一部または全部を使用しないことがあり得る。

【０３７８】

任意選択で、第１ノードは、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信し得、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用される。第１鍵更新要求において保持される第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。例えば、第３フレーム番号が２３６５である場合、フレーム番号が２３６５から開始する通信フレームの後に、前回更新された鍵が適用されること、および、第１ノードは、フレーム番号が２３６５に到達する前に、第１目標鍵を改めて決定する必要があることを示す。したがって、第１ノードは、フレーム番号が２３４５である第１通信フレームにおいて第１鍵更新要求を送信し得、第１フレーム番号２３５５は、第１鍵更新要求において第１目標鍵の開始時点を示すために使用される。通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行するためのものであり得る。したがって、フレーム番号が、前回更新された鍵のフレーム番号まで繰り返す前に、第１目標鍵が

決定され、その結果、第１目標鍵を使用することによってデータフレームが暗号化される。このように、同一のフレーム番号を有するデータフレームは、異なる鍵を使用することによって２回暗号化でき、これにより、データセキュリティを改善する。

【０３７９】

任意選択で、前回の鍵更新のプロセスにおいて、鍵開始時点を示す情報が保持されないか、または、第１ノードが以前に鍵更新を実行していない場合、第１ノードは目標フレーム番号を事前構成し得る。現在の通信フレーム番号と目標フレーム番号との間の相違点が第１閾値以下であると第１ノードが検出した場合、第１ノードは第１鍵更新要求を送信する。

【０３８０】

ステップＳ８０２：第２ノードが第１鍵更新要求を解読する。

【０３８１】

具体的には、第２ノードは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１鍵更新要求を解読し得る。

【０３８２】

ステップＳ８０３：第２ノードが第１鍵更新要求のメッセージ完全性に対する検証を実行する。

【０３８３】

任意選択で、メッセージ完全性に対する検証が失敗した場合、第２ノードは、第１ノードへの通信接続を切断し得るか、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは第１鍵更新要求を破棄し、応答しない。

【０３８４】

任意選択で、図８Ａおよび図８Ｂに示される実施形態において、第２ノードはステップＳ８０３を実行しないことがあり得る。この場合、ステップＳ８０２を実行した後に、第２ノードは続いて、ステップＳ８０４およびステップＳ８０４の後続のステップを実行し得る。

【０３８５】

ステップＳ８０４：第２ノードが第１アイデンティティ認証情報に対する検証を実行する。

【０３８６】

任意選択で、第１アイデンティティ情報に対する検証が失敗した場合、第２ノードは、第１ノードとの通信接続を切断し得るか、または、第２ノードは更新失敗インジケーション情報を第１ノードへ送信するか、または、第２ノードは、第１鍵更新要求を破棄する。

【０３８７】

任意選択で、具体的な実装プロセスにおいて、第２ノードはまず、Ｓ８０４のオペレーションを実行し、次に、Ｓ８０３のオペレーションを実行し得る。

【０３８８】

ステップＳ８０５：第１アイデンティティ認証情報に対する検証が成功した場合、第２ノードは第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成する。

【０３８９】

具体的には、アルゴリズム識別子は、鍵を生成するためのアルゴリズムを示すために使用され得る。アルゴリズム識別子は、マスター鍵、暗号化鍵、または完全性保護鍵などの鍵を生成するためのアルゴリズムの識別子を示すために使用され得る。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成することを示すために使用される。別の例では、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成することを示すために使用される。アルゴリズム識別子は代替的に、使用されるハッシュアルゴリズムの識別子または同様のものを示すために使用され得る。例えば、文字列「ＳＨＡ２５６」は、第１目標鍵を決定するために使用されるアルゴリズムがＳＨＡ２５６アルゴリズムであることを示すために使用される。アルゴリズム識別子は、第１ノードと第２ノードとの間で事前設定さ

れ得るか、または、第１ノードによって決定された後に第２ノードへ送信され得る。
【０３９０】
第２ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、およびアルゴリズム識別子ｔａｇに基づいて第１目標鍵Ｋ１を決定し得る。
【０３９１】
例えば、第２ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、およびアルゴリズム識別子ｔａｇに基づいて、鍵導出関数ＫＤＦを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ）であると決定する。
【０３９２】
任意選択で、第２ノードは更に、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、アルゴリズム識別子ｔａｇおよび鍵タイプｔｙｐｅに基づいて、鍵導出関数ＫＤＦを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ、ｔｙｐｅ）であることを決定し得、ここで、ｔｙｐｅは鍵タイプを表す。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成することを示すために使用される。別の例として、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成することを示すために使用される。
【０３９３】
任意選択で、第２ノードはまず、第１目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて中間鍵を決定し、次に、中間鍵に基づいてアルゴリズム識別子ｔａｇおよび鍵タイプｔｙｐｅの少なくとも１つを使用することによって第１目標鍵Ｋ１を決定し得る。例えば、第２ノードは、鍵導出関数ＫＤＦ１を使用することによって中間鍵Ｋｍｉｄ：Ｋｍｉｄ＝ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）を取得し、次に、中間鍵Ｋｍｉｄに基づいて鍵導出関数ＫＤＦ２を使用することによって第１目標鍵Ｋ１＝ＫＤＦ２（Ｋｍｉｄ、ｔａｇ、ｔｙｐｅ）を決定する。この解決策を本明細書においてより明確に説明するために、第１目標鍵をどのように取得するかを２つのステップを使用することによって説明することに留意されたい。実際の処理において、第１目標鍵は代替的に、１つのステップを使用することによって取得され得る。中間鍵Ｋｍｉｄは単なる中間結果である。言い換えれば、第１目標を決定する方式はＫ１＝ＫＤＦ２（ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）、ｔａｇ、ｔｙｐｅ）を満たす。
【０３９４】
ステップＳ８０６：第２ノードが第１応答メッセージを第１ノードへ送信する。
【０３９５】
本願の本実施形態において、第２目標鍵に基づいて決定された暗号化鍵を使用することによって、および／または、第２目標鍵に基づいて決定された完全性鍵を使用することによって、暗号化および／または完全性保護が第１応答メッセージに対して実行され得る。第２目標鍵は第２ノードと第１ノードとの間の共有鍵である。
【０３９６】
第１応答メッセージは第２アイデンティティ認証情報を含み、第２アイデンティティ認証情報は第２ノードのアイデンティティを認証するために使用される。任意選択で、第２アイデンティティ認証情報は、第１ノードと第２ノードとの間の第１共有鍵を使用することによって生成され得る。任意選択で、第１応答メッセージは更に乱数値ＮＯＮＣＥｓを含む。
【０３９７】
本願の本実施形態において、第２アイデンティティ認証情報を生成するためのアルゴリズムは暗号アルゴリズムであり得る。暗号アルゴリズムがＨＭＡＣである例において、生成された第２アイデンティティ認証情報ＡＵＴＨｓは、ＡＵＴＨｓ＝ＨＭＡＣ（ＰＳＫ、ＮＯＮＣＥｓ）として表され得、パラメータのシーケンスは異なり得る。当然、第１応答メッセージが乱数値ＮＯＮＣＥｓなどのパラメータを含むとき、第２ノードは、第２アイデンティティ認証情報ＡＵＴＨｓを生成するためにこれらのパラメータを使用しないことがあり得る。
【０３９８】

任意選択で、具体的な実装プロセスにおいて、第２ノードはまずＳ８０６のオペレーションを実行し、次に、Ｓ８０５のオペレーションを実行し得る。

【０３９９】

ステップＳ８０７：第１ノードが第１応答メッセージを解読する。

【０４００】

具体的には、第１ノードは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって第１応答メッセージを解読し得る。

【０４０１】

ステップＳ８０８：第１ノードが第１応答メッセージのメッセージ完全性に対する検証を実行する。

【０４０２】

具体的には、第１アイデンティティ認証情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第１ノードによって生成される。したがって、第２ノードは、第１共有鍵に基づいて、第１アイデンティティ認証情報が正確かどうかを検証し得る。

【０４０３】

任意選択で、図８Ａおよび図８Ｂに示される実施形態において、第１ノードはステップＳ８０８を実行しないことがあり得る。この場合、ステップＳ８０７を実行した後に、第１ノードは続いて、ステップＳ８０９およびステップＳ８０９の後続のステップを実行し得る。

【０４０４】

ステップＳ８０９：第１ノードが第２アイデンティティ認証情報に対して検証を実行する。

【０４０５】

具体的には、第２アイデンティティ情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第２ノードによって生成される。したがって、第１ノードは、第１共有鍵に基づいて、第２アイデンティティ認証情報が正確かどうかを検証し得る。

【０４０６】

任意選択の解決策において、プロトコルは、第１ノードが特定のパラメータを使用して第１アイデンティティ認証情報を生成すること、したがって、第２ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第１アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。例えば、第１アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成される。したがって、第２ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第１アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。

【０４０７】

例えば、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫに基づくＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証が成功する。

【０４０８】

別の例として、第１鍵ネゴシエーションパラメータが新規パラメータｆｒｅｓｈを含み、かつ、第１アイデンティティ認証情報ＡＵＴＨｍがＨＭＡＣ（ＰＳＫ、ｆｒｅｓｈ）である場合、第２ノードは、第２ノードと第１ノードとの間の事前共有鍵ＰＳＫおよび新規パラメータｆｒｅｓｈに基づいて、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ１＝ＨＭＡＣ（ＰＳＫ、ｆｒｅｓｈ）を取得する。チェック値ｃｈｅｃｋ１がＡＵＴＨｍと同一である場合、検証は成功である。

【０４０９】

任意選択で、メッセージ完全性に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示す。したがって、第１ノードは、第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄し得る。

【０４１０】

ステップＳ８０９：第１ノードが第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行する。

【０４１１】

具体的には、第２アイデンティティ情報は、第１ノードと第２ノードとの間の第１共有鍵に基づいて第２ノードによって生成される。したがって、第１ノードは、第１共有鍵に基づいて、第２アイデンティティ認証情報が正確かどうかを検証し得る。

【０４１２】

任意選択の解決策において、プロトコルは、第２ノードが特定のパラメータを使用して第２アイデンティティ認証情報を生成すること、したがって、第１ノードも同一のパラメータを使用して、検証に使用されるアイデンティティ認証情報を生成する必要があることを規定する。検証に使用されるアイデンティティ認証情報が第２アイデンティティ認証情報と同一である場合、検証が成功したとみなされる。

【０４１３】

例えば、第２アイデンティティ認証情報は、ＨＭＡＣを使用することによって生成され得る。したがって、第１ノードは、ＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２とも称される、検証に使用されるアイデンティティ認証情報を生成し、次に、検証に使用されるアイデンティティ認証情報を使用することによって、第２アイデンティティ認証情報が正確かどうかを検証し得る。以下では説明のために例を用いる。

【０４１４】

例えば、第２アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。

【０４１５】

別の例として、第１アイデンティティ認証情報ＡＵＴＨｓがＨＭＡＣ（ＰＳＫ、ＮＯＮＣＥｓ）である場合、第１ノードは、第１ノードと第２ノードとの間の事前共有鍵ＰＳＫ、ならびに、第１応答メッセージにおける乱数値ＮＯＮＣＥｓに基づいてＨＭＡＣを使用することによって、チェック値ｃｈｅｃｋ２＝ＨＭＡＣ（ＰＳＫ、ＮＯＮＣＥｓ）を取得する。チェック値ｃｈｅｃｋ２がＡＵＴＨｓと同一である場合、検証は成功である。

【０４１６】

任意選択で、第２アイデンティティ認証情報に対する検証が失敗した場合、第１ノードは、第２ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第２ノードへ送信し得るか、または、第１応答メッセージを破棄し得る。

【０４１７】

任意選択で、具体的な実装プロセスにおいて、第１ノードはまず、Ｓ８０９のオペレーションを実行し、次に、Ｓ８０８のオペレーションを実行し得る。

【０４１８】

ステップＳ８１０：第２アイデンティティ認証情報に対する検証が成功した場合、第１ノードは第２目標鍵および新規パラメータに基づいて第１目標鍵を生成する。

【０４１９】

具体的には、アルゴリズム識別子は、鍵を生成するためのアルゴリズムを示すために使用され得る。アルゴリズム識別子は、マスター鍵、暗号化鍵、または完全性保護鍵などの鍵を生成するためのアルゴリズムの識別子を示すために使用され得る。例えば、文字列「ｅｎｃｒｙｐｔｉｏｎ」は、暗号化鍵を生成することを示すために使用される。別の例では、文字列「ｉｎｔｅｇｒｉｔｙ」は、完全性保護鍵を生成することを示すために使用さ

れる。アルゴリズム識別子は代替的に、使用されるハッシュアルゴリズムの識別子または同様のものを示すために使用され得る。例えば、文字列「ＳＨＡ２５６」は、第１目標鍵を決定するために使用されるアルゴリズムがＳＨＡ２５６アルゴリズムであることを示すために使用される。アルゴリズム識別子は第１ノードと第２ノードとの間で事前設定され得るか、または、第１ノードによって決定され得る。

【０４２０】

第１ノードは、第２目標鍵Ｋ２、新規パラメータｆｒｅｓｈ、およびアルゴリズム識別子ｔａｇに基づいて、ＫＤＦアルゴリズムを使用することによって、第１目標鍵Ｋ１がＫ１＝ＫＤＦ（Ｋ２、ｆｒｅｓｈ、ｔａｇ）であることを決定し得る。

【０４２１】

任意選択で、第１ノードはまず、第１目標鍵Ｋ２および新規パラメータｆｒｅｓｈに基づいて中間鍵を決定し、次に、中間鍵に基づいてアルゴリズム識別子ｔａｇおよび鍵タイプｔｙｐｅの少なくとも１つを使用することによって第１目標鍵Ｋ１を決定し得る。例えば、第１ノードは、鍵導出関数ＫＤＦ１を使用することによって中間鍵Ｋｍｉｄ：Ｋｍｉｄ＝ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）を取得し、次に、中間鍵Ｋｍｉｄに基づいて、鍵導出関数ＫＤＦ２を使用することによって、第１目標鍵Ｋ１＝ＫＤＦ２（Ｋｍｉｄ、ｔａｇ、ｔｙｐｅ）を決定する。ＫＤＦ１およびＫＤＦ２は同一の鍵導出関数であり得るか、または、異なる鍵導出関数であり得る。本明細書において本解決策をより明確に説明するために、第１目標鍵をどのように取得するかは、２つのステップを使用することによって説明されることに留意されたい。実際の処理において、第１目標鍵は代替的に、１つのステップを使用することによって取得され得る。中間鍵Ｋｍｉｄは中間結果に過ぎない。言い換えれば、第１目標を決定する方式は、Ｋ１＝ＫＤＦ２（ＫＤＦ１（Ｋ２、ｆｒｅｓｈ）、ｔａｇ、ｔｙｐｅ）を満たす。

【０４２２】

任意選択で、第１目標鍵は、第１ノードと第２ノードとの間の共有鍵に適用され得、マスター鍵、セッション鍵などを含む。図８Ａおよび図８Ｂにおいて説明される方法では、鍵更新プロセスにおいて、第１ノードおよび第２ノードは第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、メッセージを他のノードから受信した後に、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて、第２目標鍵、新規パラメータ、およびアルゴリズム識別子に基づいて鍵を更新し、第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０４２３】

任意選択で、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される実施形態において、第１ノードによって送信された第１鍵更新要求は、第１アイデンティティ認証情報を保持しないことがあり得る。それに対応して、第２ノードは、第１アイデンティティ情報に対する検証を実行するプロセスを実行しないことがあり得る。同様に、第１応答メッセージは第２アイデンティティ認証情報を保持しないことがあり得る。それに対応して、第２ノードは、第２アイデンティティ認証情報に対する検証を実行するプロセスを実行しないことがあり得る。この場合、第１鍵更新要求は、第２目標鍵（または第２目標鍵から導出されたセッション鍵）を使用することによって暗号化され、双方のアイデンティティを認証する。

【０４２４】

可能な解決策において、第１ノードおよび第２ノードはマスター鍵およびセッション鍵を含む。セッション鍵が、マスター鍵に基づいて決定された鍵である場合、マスター鍵が失効したとき、マスター鍵は、図６Ａおよび図６Ｂまたは図７Ａおよび図７Ｂに示される鍵更新方法を使用することによって更新され得る。マスター鍵が更新されるので、マスター鍵に基づいて決定されたセッション鍵も更新される必要がある。したがって、第１ノー

ドおよび第２ノードは、図８Ａおよび図８Ｂに示される鍵更新方法を使用することによってセッション鍵を更新し得る。

【０４２５】

本願の実施形態における方法は上で詳細に説明される。本願の実施形態における装置が下に提供される。

【０４２６】

図９は、本願の実施形態による装置９０の概略構造図である。装置９０は、データ受信／送信能力を有する電子デバイスであり得るか、または、データ受信／送信能力を有する電子デバイスにおける、チップまたは集積回路などのコンポーネントであり得る。装置９０は、送信ユニット９０１、受信ユニット９０２、検証ユニット９０３、および決定ユニット９０４を含み得る。ユニットは以下のように説明される。

【０４２７】

送信ユニット９０１は、第１鍵更新要求を第２ノードへ送信するよう構成され、ここで、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される。

【０４２８】

受信ユニット９０２は、第１応答メッセージを第２ノードから受信するよう構成され、ここで、第１応答メッセージは第２アイデンティティ認証情報を含む。

【０４２９】

検証ユニット９０３は、第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するよう構成される。

【０４３０】

決定ユニット９０４は、第２アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するよう構成される。

【０４３１】

鍵更新プロセスにおいて、上述の装置９０および第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０４３２】

本明細書において、上述の複数のユニットの分割は、単に機能に基づく論理的分割であり、装置９０の特定の構造に限定する意図は無いことを留意されたい。特定の実装において、いくつかの機能モジュールは、より細かい機能モジュールに細分割され得、いくつかの機能モジュールは、１つの機能モジュールに組み合わされ得る。しかしながら、機能モジュールが細分割されるか、または、組み合わされるかにかかわらず、鍵更新プロセスにおける装置９０によって実行される概略的手順は同一である。例えば、上述の複数のユニットは、通信ユニットおよび処理ユニットとして単純化され得る。通信ユニットは、送信ユニット９０１および受信ユニット９０２の１または複数の機能を実装するよう構成され、処理ユニットは、検証ユニット９０３および決定ユニット９０４の１または複数の機能を実装するよう構成される。通常、各ユニットは、それぞれのプログラムコード（またはプログラム命令）に対応する。ユニットに対応するプログラムコードがプロセッサ上で実行されるとき、ユニットは、対応する手順を実行して、対応する関数を実装する。

【０４３３】

可能な実装において、第１鍵更新要求は第１更新時点および、第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【０４３４】

従来の鍵更新プロセスにおいて、鍵更新時点は、プロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願において提供される装置９０は、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、第２ノードへの更新時間および／または有効期間を示し得、その結果、第１目標鍵を適宜に有効化することができる。

【０４３５】

更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は、第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０４３６】

例えば、第１鍵更新要求において保持される第１フレーム番号は２３４５であり、第１フレーム番号は、第１目標鍵が、フレーム番号２３４５から開始する通信フレームの後に適用されることを示し得る。

【０４３７】

更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【０４３８】

従来の鍵更新プロセスにおいて、鍵更新時点が構成される。したがって、古い鍵が失効するときに新しい鍵が更新される。古い鍵が失効したので、鍵更新中に暗号化プロセスが保留される必要があり、暗号化プロセスは、鍵更新が完了した後に再開される。しかしながら、暗号化プロセスの保留および暗号化プロセスの再開は鍵更新効率に影響を与え、暗号化プロセスの保留はセキュリティに影響を与える。しかしながら、本願の装置９０において、古い鍵が失効していないので、鍵更新中に暗号化プロセスは保留される必要が無く、これにより、鍵更新効率を改善しデータセキュリティを改善する。

【０４３９】

更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、決定ユニット９０４は、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。

【０４４０】

更に別の可能な実装において、第１鍵ネゴシエーションパラメータは、新規パラメータを含み、決定ユニット９０４は、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。

【０４４１】

第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）な

どを含み得る。
【０４４２】
更に別の可能な実装において、第１目標鍵は装置９０のマスター鍵である。
【０４４３】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、決定ユニット９０４は、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、ここで、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。
【０４４４】
更に別の可能な実装において、第１目標鍵は、装置９０の完全性保護鍵または暗号化鍵である。
【０４４５】
更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって暗号化され、および／または、完全性保護が、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。
【０４４６】
従来の鍵更新方法は、古い鍵が失効するときに鍵を更新することであることが理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において提供される装置９０は、鍵が失効する前に第１目標鍵を決定し得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。
【０４４７】
更に別の可能な実装において、送信ユニット９０１は、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信するよう構成され、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。
【０４４８】
通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行することであり得る。したがって、フレーム番号が前回更新された鍵のフレーム番号まで繰り返す前に第１目標鍵が決定され、その結果、データフレームが、第１目標鍵を使用することによって暗号化される。このように、同一のフレーム番号を有するデータフレームが、異なる鍵を使用することによって２回暗号化され得、これにより、データセキュリティを改善する。代替的解決策において、第１鍵更新要求は、第１フレーム番号の代わりにＭＡＣシリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮはＭビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。代替的に、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号はまた、ＭＡＣ　ＳＮ、すなわち、第３フレーム番号の示すために使用される複数のビットの一部によって示されるＭＡＣ　ＳＮで置き換えられ得る。この代替的解決策において、第１フレーム番号、第２フレーム番号、および第３フレーム番号の間の値関係は変化しないままである。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代

替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０４４９】

更に別の可能な実装において、通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む。

【０４５０】

更に別の可能な実装において、第２アイデンティティ情報に対する検証が失敗した場合、送信ユニット９０１および受信ユニット９０２は、第２ノードへの通信接続を切断するか、または、送信ユニット９０１を使用することによって、更新失敗情報を第２ノードへ送信する。

【０４５１】

第２アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、上述の装置９０は、第２ノードへの通信接続を切断し得るか、または、更新失敗情報を第２ノードへ送信し得、その結果、鍵更新を実行する必要があるノードに対するアクセス要求が再初期化され、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０４５２】

更に別の可能な実装において、検証ユニット９０３は更に、第１応答メッセージに対する完全性検証を実行するよう構成され、完全性検証が成功した場合、続いて、第１共有鍵を使用することによって、第２アイデンティティ認証情報に対する検証を実行するステップを実行し、完全性検証が失敗した場合、送信ユニット９０１および受信ユニット９０２は第２ノードへの通信接続を切断するか、または、送信ユニット９０１を使用することによって、更新失敗情報を第２ノードへ送信するか、もしくは、更新失敗情報を第２ノードへ送信し得る。

【０４５３】

装置９０は、アイデンティティ情報に対する検証を実行する前に、まず、第１応答メッセージに対する完全性検証を実行し、第１応答メッセージにおける情報が改ざんされていないと決定し得る。完全性検証が失敗した場合、第１応答情報におけるデータは改ざんされ、鍵を更新できないことを示す。したがって、装置９０は、第２ノードへの通信接続を切断するか、または、更新失敗情報を第２ノードへ送信し、その結果、装置９０は、鍵更新を実行する必要があるノードに再アクセスし、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０４５４】

各ユニットの実装については、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における対応する説明を参照することに留意されたい。装置９０は、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第１ノードである。

【０４５５】

図１０は、本願の実施形態による装置１００の概略構造図である。装置１００は、データ受信／送信能力を有する電子デバイスであり得るか、または、データ受信／送信能力を有する電子デバイスにおけるチップまたは集積回路などのコンポーネントであり得る。装置１００は受信ユニット１００１、検証ユニット１００２、決定ユニット１００３、および送信ユニット１００４を含み得る。ユニットは以下のように説明される。

【０４５６】

受信ユニット１００１は、第１鍵更新要求を第１ノードから受信するよう構成され、ここで、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む。

【０４５７】

検証ユニット１００２は、第１共有鍵を使用することによって第１アイデンティティ認

証情報に対する検証を実行するよう構成される。

【０４５８】

決定ユニット１００３は、第１アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するよう構成される。

【０４５９】

送信ユニット１００４は、第１応答メッセージを第１ノードへ送信するよう構成され、ここで、第１応答メッセージは第２アイデンティティ認証情報を含み、第２アイデンティティ認証情報は、第１共有鍵を使用することによって生成される。

【０４６０】

元のセッション鍵が失効する前に、上述の装置１００および第１ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０４６１】

本明細書において、上述の複数のユニットの分割は、単に機能に基づく論理的分割であり、装置１００の特定の構造に限定する意図は無いことに留意されたい。特定の実装において、いくつかの機能モジュールは、より細かい機能モジュールに細分割され得、いくつかの機能モジュールは、１つの機能モジュールに組み合わされ得る。しかしながら、機能モジュールが細分割されるか、または、組み合わされるかにかかわらず、鍵更新プロセスにおける装置１００によって実行される概略的手順は同一である。例えば、上述の複数のユニットは、通信ユニットおよび処理ユニットとして単純化され得る。通信ユニットは、受信ユニット１００１および送信ユニット１００４の機能を実装するよう構成され、処理ユニットは、検証ユニット１００２および決定ユニット１００３の１または複数の機能を実装するよう構成される。通常、各ユニットは、それぞれのプログラムコード（またはプログラム命令）に対応する。ユニットに対応するプログラムコードがプロセッサ上で実行されるとき、ユニットは、対応する手順を実行して、対応する関数を実装する。

【０４６２】

可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【０４６３】

従来の鍵更新プロセスにおいて、鍵更新時点は、プロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願における鍵更新方法において、第１ノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、更新時点および／または有効期間を装置１００に示し得、その結果、第１目標鍵を適宜に有効化できる。

【０４６４】

更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は、第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持

され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０４６５】

例えば、第１鍵更新要求において保持される第１フレーム番号は２３４５であり、第１フレーム番号は、第１目標鍵が、フレーム番号２３４５から開始する通信フレームの後に適用されることを示し得る。

【０４６６】

更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。

【０４６７】

更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは第２鍵ネゴシエーションアルゴリズムパラメータを含み、決定ユニット１００３は、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。

【０４６８】

更に別の可能な実装において、第１鍵ネゴシエーションパラメータは、新規パラメータを含み、決定ユニット１００３は、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。

【０４６９】

第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。

【０４７０】

更に別の可能な実装において、第１目標鍵は装置１００のマスター鍵である。

【０４７１】

更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、決定ユニット１００３は、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、ここで、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムを識別するために使用される。

【０４７２】

更に別の可能な実装において、第１目標鍵は装置１００の完全性保護鍵または暗号化鍵である。

【０４７３】

更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって暗号化され、および／または、完全性保護が、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【０４７４】

従来の鍵更新方法は、古い鍵が失効したときに鍵を更新することであると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、装置１００は、鍵が失効する前に第１目標鍵を決定し得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、こ

れにより、データセキュリティを改善する。
【０４７５】
更に別の可能な実装において、送信ユニット１００４は更に、第１アイデンティティ情報に対する検証が失敗した場合に、装置１００が第１ノードへの通信接続を切断する、または、更新失敗インジケーション情報を第１ノードへ送信するよう構成される。
【０４７６】
第１アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、装置１００は、第１ノードへの接続を切断し得るか、または、第１ノードへ更新失敗インジケーション情報を送信し得、現在の鍵プロセスを停止し、これにより、鍵更新プロセスにおける装置１００のデータセキュリティを確実にする。
【０４７７】
更に別の可能な実装において、検証ユニット１００２は更に、第１応答メッセージに対する完全性検証を実行し、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するステップを実行するよう構成され、送信ユニット１００４は更に、完全性検証が失敗した場合、装置１００が第１ノードへの通信接続を切断するか、または、更新失敗インジケーション情報を第１ノードへ送信するよう構成される。
【０４７８】
上述の装置１００は、アイデンティティ情報に対する検証を実行する前に、まず第１鍵更新要求に対する完全性検証を実行して、第１鍵更新要求における情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１鍵更新要求におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、上述の装置１００は、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。
【０４７９】
各ユニットの実装については、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における対応する説明を参照することに留意されたい。装置１００は、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第２ノードである。
【０４８０】
図１１は、本願の実施形態による装置１１０の概略構造図である。装置１１０は、データ受信／送信能力を有する電子デバイスであり得るか、または、データ受信／送信能力を有する電子デバイスにおけるチップまたは集積回路などのコンポーネントであり得る。装置１１０はメモリ１１０１、プロセッサ１１０２および通信インタフェース１１０３を含み得る。更に任意選択で、バス１１０４が更に含まれ得る。メモリ１１０１、プロセッサ１１０２および通信インタフェース１１０３はバス１１０４を通じて接続される。
【０４８１】
メモリ１１０１は記憶空間を提供するよう構成され、記憶空間は、オペレーティングシステムおよびコンピュータプログラムなどのデータを記憶し得る。メモリ１１０１には、限定されるものではないが、ランダムアクセスメモリ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ、ＲＡＭ）、リードオンリメモリ（ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＲＯＭ）、消去可能プログラマブルリードオンリメモリ（ｅｒａｓａｂｌｅ ｐｒｏｇｒａｍｍａｂｌｅ ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ、ＥＰＲＯＭ）、またはコンパクトディスクリードオンリメモリ（ｃｏｍｐａｃｔ ｄｉｓｃ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＣＤ－ＲＯＭ）が含まれる。
【０４８２】
プロセッサ１１０２は、算術演算および論理演算を実行するモジュールであり、中央処理装置（ｃｅｎｔｒａｌ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ、ＣＰＵ）、グラフィックス処理ユニット（ｇｒａｐｈｉｃｓ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ，ＧＰＵ）、また

はマイクロプロセッサユニット（ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ　ｕｎｉｔ，　ＭＰＵ）などの処理モジュールの１つまたは組み合わせであり得る。

【０４８３】

通信インタフェース１１０３は、外部デバイスによって送信されたデータを受信し、および／または、データを外部デバイスへ送信するよう構成され、イーサネット（登録商標）ケーブルなどの有線リンクインタフェースであり得、または、無線リンクインタフェース（Ｗｉ－Ｆｉ、Ｂｌｕｅｔｏｏｔｈまたは同様のもの）であり得る。任意選択で、通信インタフェースは更に、インタフェースに結合された送信機（例えば、無線周波数送信機）、受信機、または同様のものを含み得る。

【０４８４】

装置１１０におけるプロセッサ１１０２は、メモリ１１０１に記憶されたコンピュータプログラムコードを読み取り、以下のオペレーション、すなわち、通信インタフェース１１０３を通じて第１鍵更新要求を第２ノードへ送信することであって、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、こと、通信インタフェース１１０４を通じて、第１応答メッセージを第２ノードから受信することであって、第１応答メッセージは第２アイデンティティ認証情報を含む、こと、第１共有鍵を使用することによって、第２アイデンティティ認証情報に対する検証を実行すること、および、第２アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することを実行するよう構成される。

【０４８５】

鍵更新プロセスにおいて、上述の装置１１０および第２ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０４８６】

可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【０４８７】

従来の鍵更新プロセスにおいて、鍵更新時点は、プロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願において提供される装置１１０は、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、第２ノードへの更新時点および／または有効期間を示し得、その結果、第１目標鍵を適宜に有効化することができる。

【０４８８】

更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は、第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０４８９】
例えば、第１鍵更新要求において保持される第１フレーム番号は２３４５であり、第１フレーム番号は、第１目標鍵が、フレーム番号２３４５から開始する通信フレームの後に適用されることを示し得る。
【０４９０】
更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。
【０４９１】
従来の鍵更新プロセス、鍵更新時点が構成される。したがって、古い鍵が失効するとき新しい鍵が更新される。古い鍵が失効したので、鍵更新中に暗号化プロセスが保留される必要があり、暗号化プロセスは、鍵更新が完了した後に再開される。しかしながら、暗号化プロセスの保留および暗号化プロセスの再開は鍵更新効率に影響を与え、暗号化プロセスの保留はセキュリティに影響を与える。しかしながら、本願において提供される装置１１０において、古い鍵が失効していないので、鍵更新中に暗号化プロセスは保留される必要が無く、これにより、鍵更新効率を改善しデータセキュリティを改善する。
【０４９２】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサ１１０２は具体的には、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。
【０４９３】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサ１１０２は具体的には、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。
【０４９４】
第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。
【０４９５】
更に別の可能な実装において、第１目標鍵は装置１１０のマスター鍵である。
【０４９６】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサ１１０２は具体的には、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。
【０４９７】
更に別の可能な実装において、第１目標鍵は、装置１１０の完全性保護鍵または暗号化鍵である。
【０４９８】
更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも

１つは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって暗号化され、および／または、完全性保護が、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【０４９９】

従来の鍵更新方法は、古い鍵が失効したときに鍵を更新することであると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、装置１１０は、鍵が失効する前に第１目標鍵を決定し得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。

【０５００】

更に別の可能な実装において、通信インタフェース１１０３は、第１通信フレームを使用することによって、第１鍵更新要求を第２ノードへ送信し、ここで、第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求において保持される第３フレーム番号より小さく、第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、第１フレーム番号は、第２フレーム番号より大きく、第３フレーム番号より小さい。

【０５０１】

通信プロセスにおいて通信フレームに対してセキュリティ保護が実行されるとき、使用される暗号化方法は、フレーム番号および前回更新された鍵に基づいて暗号化を実行することであり得る。したがって、フレーム番号が前回更新された鍵のフレーム番号まで繰り返す前に第１目標鍵が決定され、その結果、データフレームが、第１目標鍵を使用することによって暗号化される。このように、同一のフレーム番号を有するデータフレームが、異なる鍵を使用することによって２回暗号化され得、これにより、データセキュリティを改善する。

【０５０２】

代替的解決策において、第１鍵更新要求は、第１フレーム番号の代わりにＭＡＣシリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮはＭビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。代替的に、前回の鍵更新中に使用される鍵更新要求において保持される第３フレーム番号はまた、ＭＡＣ　ＳＮ、すなわち、第３フレーム番号の示すために使用される複数のビットの一部によって示されるＭＡＣ　ＳＮで置き換えられ得る。この代替的解決策において、第１フレーム番号、第２フレーム番号、および第３フレーム番号の間の値関係は変化しないままである。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０５０３】

更に別の可能な実装において、通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む。

【０５０４】

更に別の可能な実装において、プロセッサ１１０２は更に、第２アイデンティティ情報に対する検証が失敗した場合、第２ノードへの通信接続を切断するか、または、通信インタフェース１１０３を通じて更新失敗情報を第２ノードへ送信するよう通信インタフェース１１０３に示すよう構成される。

【０５０５】

第２アイデンティティ認証情報に対する検証が失敗した場合、第２ノードのアイデンティティが信用できないことを示すことが分かり得る。したがって、上述の装置１１０は、第２ノードへの通信接続を切断し得るか、または、更新失敗情報を第２ノードへ送信し得、その結果、鍵更新を実行する必要があるノードに対するアクセス要求が再初期化され、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０５０６】

更に別の可能な実装において、プロセッサ１１０２は更に、第２ノードから第１応答メッセージを受信した後に、第１応答メッセージに対する完全性検証を実行し、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第２アイデンティティ認証情報に対する検証を実行するステップを実行するよう構成され、プロセッサ１１０２は更に、完全性検証が失敗した場合、第２ノードへの通信接続を切断するか、または、通信インタフェース１１０３を通じて更新失敗情報を第２ノードへ送信するよう通信インタフェース１１０３に示すよう構成される。

【０５０７】

情報が改ざんされているかどうかを決定するために完全性検証が実行され得ることが分かり得る。したがって、アイデンティティ情報に対する検証を実行する前に、上述の装置１１０はまず、第１応答メッセージに対する完全性検証を実行して、第１応答メッセージにおける情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１応答情報におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、装置１１０は、第２ノードへの通信接続を切断するか、または、更新失敗情報を第２ノードへ送信し、その結果、装置１１０は、鍵更新を実行する必要があるノードに再アクセスし、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。

【０５０８】

各ユニットの実装については、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における対応する説明を参照することに留意されたい。ノード１０は、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第１ノードである。

【０５０９】

図１２は、本願の実施形態による装置１２０の概略構造図である。装置１２０は、データ受信／送信能力を有する電子デバイスであり得るか、または、データ受信／送信能力を有する電子デバイスにおけるチップまたは集積回路などのコンポーネントであり得る。装置１２０は、メモリ１２０１、プロセッサ１２０２、および通信インタフェース１２０３を含み得る。更に任意選択で、バス１２０４が更に含まれ得る。メモリ１２０１、プロセッサ１２０２、および通信インタフェース１２０３はバス１２０４を通じて接続される。

【０５１０】

メモリ１２０１は、記憶空間を提供するよう構成され、記憶空間はオペレーティングシステムおよびコンピュータプログラムなどのデータを記憶し得る。メモリ１２０１には、限定されるものではないが、ランダムアクセスメモリ（ｒａｎｄｏｍ ａｃｃｅｓｓ ｍｅｍｏｒｙ、ＲＡＭ）、リードオンリメモリ（ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＲＯＭ）、消去可能プログラマブルリードオンリメモリ（ｅｒａｓａｂｌｅ ｐｒｏｇｒａｍｍａｂｌｅ ｒｅａｄ ｏｎｌｙ ｍｅｍｏｒｙ、ＥＰＲＯＭ）、またはコンパクトディスクリードオンリメモリ（ｃｏｍｐａｃｔ ｄｉｓｃ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ、ＣＤ－ＲＯＭ）が含まれる。

【０５１１】

プロセッサ１２０２は、算術演算および論理演算を実行するモジュールであり、中央処理装置（ｃｅｎｔｒａｌ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ、ＣＰＵ）、グラフィックス処理ユニット（ｇｒａｐｈｉｃｓ ｐｒｏｃｅｓｓｉｎｇ ｕｎｉｔ，ＧＰＵ）、またはマイクロプロセッサユニット（ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ ｕｎｉｔ，ＭＰＵ）などの処理モジュールの１つまたは組み合わせであり得る。

【０５１２】

通信インタフェース１２０３は、外部デバイスによって送信されたデータを受信し、および／または、データを外部デバイスへ送信するよう構成され、イーサネットケーブルなどの有線リンクインタフェースであり得、または、無線リンクインタフェース（Ｗｉ－Ｆｉ、Ｂｌｕｅｔｏｏｔｈまたは同様のもの）であり得る。任意選択で、通信インタフェースは更に、インタフェースに結合された送信機（例えば、無線周波数送信機）、受信機、または同様のものを含み得る。

【０５１３】

デバイス１２０におけるプロセッサ１２０２は、メモリ１２０１に記憶されたコンピュータプログラムコードを読み取り、以下のオペレーション、すなわち、通信インタフェース１２０３を通じて第１鍵更新要求を第２ノードへ送信することであって、第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、こと、通信インタフェース１２０３を通じて、第１応答メッセージを第２ノードから受信することであって、第１応答メッセージは第２アイデンティティ認証情報を含む、こと、第１共有鍵を使用することによって、第２アイデンティティ認証情報に対する検証を実行すること、および、第２アイデンティティ認証情報に対する検証が成功した場合、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定することを実行するよう構成される。

【０５１４】

元のセッション鍵が失効する前に、上述の装置１２０および第１ノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する。１つのノードは、他のノードからメッセージを受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に初めて第鍵ネゴシエーションパラメータに基づいて鍵を更新して第１目標鍵を取得する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、鍵更新プロセスにおけるデータセキュリティを改善する。

【０５１５】

可能な実装において、第１鍵更新要求は、第１更新時点および第１目標鍵の有効期間の少なくとも１つを示すために使用される。

【０５１６】

従来の鍵更新プロセスにおいて、鍵更新時点がプロトコルにおいて事前定義され、柔軟に選択できない。しかしながら、本願において、第１ノードは、第１目標鍵の更新時点および／または第１目標鍵の有効期間をカスタマイズし、更新時点および／または有効期間を装置１２０に示し得、その結果、第１目標鍵を適宜に有効化できる。

【０５１７】

更に別の可能な実装において、第１鍵更新要求は第１フレーム番号を含み、第１鍵更新要求は、第１フレーム番号を使用することによって第１更新時点を示す。第１フレーム番号は、複数のビット、例えばＦビットを使用することによって示される。代替的に、第１鍵更新要求は、媒体アクセス制御シリアル番号（ＭＡＣ　ＳＮ）を含み、ＭＡＣ　ＳＮは、Ｍビットを使用することによって示され、ＭビットはＦビットの一部であり、ＭはＦより小さい。具体的には、第１フレーム番号を示すために使用される複数のビットは、２つの部分、すなわち、上位部分および下位部分を含む。下位部分は、ＭＡＣ　ＳＮを示すために使用されるＭビットである。上位部分は、Ｎビットを使用することによって示される。任意選択で、Ｎビットは、ハイパーフレーム番号を示すために使用される複数のビットである。この代替的な方式において、できるだけ少ない情報は、鍵更新要求において保持され得、これにより、シグナリング消費を低減し、通信効率を改善する。

【０５１８】

例えば、第１鍵更新要求において保持される第１フレーム番号は２３４５であり、第１フレーム番号は、第１目標鍵が、フレーム番号２３４５から開始する通信フレームの後に適用されることを示し得る。

【０５１９】
更に別の可能な実装において、第１目標鍵は、第１更新時点から開始する第１目標鍵の有効期間内に適用される。
【０５２０】
従来の鍵更新プロセスにおいて、鍵更新時点が構成される。したがって、古い鍵が失効するとき、新しい鍵が更新される。古い鍵が失効したので、鍵更新中に暗号化プロセスが保留される必要があり、暗号化プロセスは、鍵更新が完了した後に再開される。しかしながら、暗号化プロセスの保留および暗号化プロセスの再開は鍵更新効率に影響を与え、暗号化プロセスの保留はセキュリティに影響を与える。しかしながら、本願において提供される装置１２０において、古い鍵が失効していないので、鍵更新中に暗号化プロセスは保留される必要が無く、これにより、鍵更新効率を改善しデータセキュリティを改善する。
【０５２１】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサ１２０２は具体的には、第１鍵ネゴシエーションアルゴリズムパラメータおよび第２鍵ネゴシエーションアルゴリズムパラメータに基づいて第１目標鍵を生成するよう構成される。
【０５２２】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサ１２０２は具体的には、第２目標鍵および新規パラメータに基づいて第１目標鍵を生成するよう構成される。
【０５２３】
第２目標鍵は第１ノードと第２ノードとの間の共有鍵であり得、マスター鍵、セッション鍵、事前共有鍵ＰＳＫなどを含む。加えて、第１目標鍵は、第２目標鍵および新規パラメータに基づいて、鍵導出アルゴリズムＫＤＦを使用することによって生成され得る。例えば、秘密値Ｋｅｙを使用することによって導出された新しい鍵ＤＫは、ＤＫ＝ＫＤＦ（Ｋｅｙ、ｆｒｅｓｈ）として表現され得、ここで、ｆｒｅｓｈは新規パラメータであり、更新に使用されるパラメータであり、カウンタ値（ｃｏｕｎｔｅｒ）、シリアル番号（ｎｕｍｂｅｒ）、ランダム値（ｒａｎｄ）、フレーム番号（ｆｒａｍｅ　ｎｕｍｂｅｒ）などを含み得る。
【０５２４】
更に別の可能な実装において、第１目標鍵は装置１２０のマスター鍵である。
【０５２５】
更に別の可能な実装において、第１鍵ネゴシエーションパラメータは新規パラメータを含み、第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するオペレーションにおいて、プロセッサ１２０２は具体的には、第２目標鍵、新規パラメータおよびアルゴリズム識別子に基づいて第１目標鍵を生成するよう構成され、アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される。
【０５２６】
更に別の可能な実装において、第１目標鍵は、装置１２０の完全性保護鍵または暗号化鍵である。
【０５２７】
更に別の可能な実装において、第１鍵更新要求および第１応答メッセージの少なくとも１つは、第２目標鍵に基づいて決定された暗号化鍵を使用することによって暗号化され、および／または、完全性保護が、第２目標鍵に基づいて決定された完全性保護鍵を使用することによって、第１鍵更新要求および第１応答メッセージの少なくとも１つに対して実行される。

【０５２８】
従来の鍵更新方法は、古い鍵が失効するときに鍵を更新することであると理解され得る。第２目標鍵は失効したので、暗号化および完全性保護は、新しい鍵を決定するプロセスにおいて実行されない。しかしながら、本願の本実施形態において、第１目標鍵は、鍵が失効する前に決定され得る。したがって、第１鍵更新要求および第１応答メッセージは、第２目標鍵に基づいて決定された鍵を使用することによって暗号化され得、これにより、データセキュリティを改善する。
【０５２９】
更に別の可能な実装において、プロセッサ１２０２は更に、第１アイデンティティ情報に対する検証が失敗した場合に、第１ノードへの通信接続を切断する、または、通信インタフェース１２０３を通じて更新失敗インジケーション情報を第１ノードへ送信するよう通信インタフェース１２０３に示すよう構成される。
【０５３０】
第１アイデンティティ認証情報に対する検証が失敗した場合、装置１２０は、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、現在の鍵プロセスを停止し、これにより、鍵更新プロセスのノードのデータセキュリティを確実にすることが分かり得る。
【０５３１】
更に別の可能な実装において、プロセッサ１２０２は更に、第１鍵更新要求を第１ノードから受信した後、第１鍵更新要求に対する完全性検証を実行し、完全性検証が成功した場合、続いて第１共有鍵を使用することによって第１アイデンティティ認証情報に対する検証を実行するステップを実行するよう構成され、プロセッサ１２０２は更に、完全性検証が失敗した場合、第１ノードへの接続を切断するか、または、通信インタフェース１２０３を通じて更新失敗インジケーション情報を第１ノードへ送信するよう通信インタフェース１２０３に示すよう構成される。
【０５３２】
上述の装置１２０は、アイデンティティ情報に対する検証を実行する前に、まず第１鍵更新要求に対する完全性検証を実行して、第１鍵更新要求における情報が改ざんされていないことを決定する。完全性検証が失敗した場合、第１鍵更新要求におけるデータが改ざんされ、鍵を更新できないことを示す。したがって、上述の装置１２０は、第１ノードへの接続を切断し得るか、または、更新失敗インジケーション情報を第１ノードへ送信し得、これにより、鍵更新プロセスにおけるデータセキュリティを確実にする。
【０５３３】
各ユニットの実装については、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における対応する説明を参照することに留意されたい。装置１２０は、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第１ノードである。
【０５３４】
本願の実施形態がさらに、コンピュータ可読記憶媒体を提供する。このコンピュータ可読記憶媒体は、コンピュータプログラムを記憶する。コンピュータプログラムが１または複数のプロセッサ上で実行されるとき、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の一実施形態における方法が実行される。
【０５３５】
本願の実施形態は更に、チップシステムを提供する。チップシステムは少なくとも１つのプロセッサ、メモリおよびインタフェース回路を含む。インタフェース回路は、少なくとも１つのプロセッサについての情報入力／出力を提供するよう構成され、少なくとも１つのメモリはコンピュータプログラムを記憶し、コンピュータプログラムが１または複数のプロセッサ上で実行されるとき、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における鍵更新方法が実行される。
【０５３６】

本願のある実施形態は、スマート運転席製品を更に提供する。スマート運転席製品は、第１ノード（例えば、自動車運転席ドメインコントローラＣＤＣ）を含み、第１ノードは、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第１ノードである。更に、車両は第２ノード（例えば、カメラ、スクリーン、マイク、スピーカ、レーダ、電子鍵、およびキーレスエントリならびに起動システムコントローラなどのモジュールの少なくとも１つ）を更に含み、第２ノードは、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第２ノードである。

【０５３７】

本願の実施形態は更に、車両を提供する。車両は第１ノード（例えば、自動車運転席ドメインコントローラＣＤＣ）を含む。更に、車両は第２ノード（例えば、カメラ、スクリーン、マイク、スピーカ、レーダ、電子鍵、およびキーレスエントリ、または起動システムコントローラなどのモジュールの少なくとも１つ）を更に含む。第１ノードは、図５、図６Ａ、および図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第１ノードであり、第２ノードは、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における第２ノードである。本願の実施形態は更にコンピュータプログラム製品を提供する。コンピュータプログラム製品が１または複数のプロセッサ上で実行されるとき、図５、図６Ａおよび図６Ｂ、図７Ａおよび図７Ｂ、または図８Ａおよび図８Ｂに示される任意の実施形態における鍵更新方法が実行され得る。

【０５３８】

上記に鑑み、本願の実施形態において提供される鍵更新方法によれば、鍵が更新される前に、通信の双方のノードは、第１共有鍵に基づいてアイデンティティ認証情報を生成する必要がある。１つのノードは、メッセージを他のノードから受信した後、まずアイデンティティ認証情報を使用することによって他のノードのアイデンティティを決定し、アイデンティティ認証が成功した後に鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する。この場合、盗聴者が元のセッション鍵をクラッキングした場合でも、盗聴者はアイデンティティ情報を偽造できず、これにより、中間者攻撃を回避し、データ更新プロセスにおけるデータセキュリティを改善する。

【０５３９】

簡潔に説明するために、上述した方法の複数の実施形態は、一連の動作の組み合わせとして表されていることに留意されたい。しかしながら、当業者であれば、本願によれば、いくつかのステップは、別の順序で、または同時に実行され得るので、本願は、説明された動作の順序に限定されないことを理解するはずである。当業者であれば、本明細書において説明される実施形態はすべて、例示的な実施形態に属し、関連する動作およびモジュールは必ずしも本願によって要求とされないことを更に理解するはずである。

【０５４０】

本願の実施形態による方法のステップのシーケンスは、実際の要件に基づいて、調節され、組み合わされ、または、削除され得る。

【０５４１】

本願の実施形態による装置におけるモジュールは、実際の要件に基づいて組み合わされ、分割され、削除され得る。

【０５４２】

当業者は、複数の実施形態による方法のステップの全てまたはいくつかが関連するハードウェアに命令するプログラムにより実装され得ることを理解し得る。プログラムは、コンピュータ可読記憶媒体に記憶され得る。記憶媒体には、フラッシュメモリ、リードオンリメモリ（Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙ、ＲＯＭ）、ランダムアクセスメモリ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ、ＲＡＭ）、磁気ディスク、光ディスクまたは同様のものが含まれてよい。

【０５４３】

上に開示されるものは、本願の例示的な実施形態に過ぎない。当業者であれば、上記の実施形態を実装する手順の全部または一部、および、本願の請求項に従って加えられた同等の修正は、本願の範囲内に含まれることを理解し得る。

［他の可能な項目］

（項目１）

鍵更新方法であって、

第１鍵更新要求を第２ノードへ送信する段階であって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、前記第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、段階と、

第１応答メッセージを前記第２ノードから受信する段階であって、前記第１応答メッセージは第２アイデンティティ認証情報を含む、段階と、

前記第１共有鍵を使用することによって、前記第２アイデンティティ認証情報に対する検証を実行する段階と、

前記第２アイデンティティ認証情報に対する前記検証が成功した場合、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する段階と

を備える方法。

（項目２）

前記第１鍵更新要求は、第１更新時点および前記第１目標鍵の有効期間の少なくとも１つを示すために使用される、項目１に記載の方法。

（項目３）

前記第１鍵更新要求は第１フレーム番号または第１媒体アクセス制御ＭＡＣシリアル番号を含み、前記第１鍵更新要求は、前記第１フレーム番号または前記第１ＭＡＣシリアル番号を使用することによって前記第１更新時点を示すために使用される、項目２に記載の方法。

（項目４）

前記第１目標鍵は、前記第１更新時点から開始する前記第１目標鍵の前記有効期間内に適用される、項目２に記載の方法。

（項目５）

前記第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、前記第１応答メッセージは第２鍵ネゴシエーションアルゴリズムパラメータを更に含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、前記第１鍵ネゴシエーションアルゴリズムパラメータおよび前記第２鍵ネゴシエーションアルゴリズムパラメータに基づいて前記第１目標鍵を生成する段階を含む、項目１から４のいずれか一項に記載の方法。

（項目６）

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、第２目標鍵および前記新規パラメータに基づいて前記第１目標鍵を生成する段階を含む、項目１から４のいずれか一項に記載の方法。

（項目７）

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、第２目標鍵、前記新規パラメータおよびアルゴリズム識別子に基づいて前記第１目標鍵を生成する段階であって、前記アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される、段階を含む、項目１から４のいずれか一項に記載の方法。

（項目８）

前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つは、前記第２目標鍵に基づいて決定された前記暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、前記第２目標鍵に基づいて決定された前記完全性保護鍵を使用するこ

とによって、前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つに対して実行される、項目１から７のいずれか一項に記載の方法。

（項目９）

前記第１鍵更新要求は前記第１フレーム番号を含み、前記第１フレーム番号は、前記第１目標鍵の更新時点を示すために使用され、第１鍵更新要求を第２ノードへ送信する前記段階は、

第１通信フレームを使用することによって、前記第１鍵更新要求を前記第２ノードへ送信する段階であって、前記第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求に保持される第３フレーム番号より小さく、前記第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、前記第１フレーム番号は前記第２フレーム番号より大きく、前記第３フレーム番号より小さい、段階を含む、項目１から８のいずれか一項に記載の方法。

（項目１０）

前記通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む、項目９に記載の方法。

（項目１１）

鍵更新方法であって、

第１鍵更新要求を第１ノードから受信する段階であって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む、段階と、

第１共有鍵を使用することによって、前記第１アイデンティティ認証情報に対する検証を実行する段階と、

前記第１アイデンティティ認証情報に対する前記検証が成功した場合、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する段階と、

第１応答メッセージを前記第１ノードへ送信する段階であって、前記第１応答メッセージは第２アイデンティティ認証情報を含み、前記第２アイデンティティ認証情報は、前記第１共有鍵を使用することによって生成される、段階と

を備える方法。

（項目１２）

前記第１鍵更新要求は、第１更新時点および前記第１目標鍵の有効期間の少なくとも１つを示すために使用される、項目１１に記載の方法。

（項目１３）

前記第１鍵更新要求は第１フレーム番号または第１媒体アクセス制御ＭＡＣシリアル番号を含み、前記第１鍵更新要求は、前記第１フレーム番号または前記第１ＭＡＣシリアル番号を使用することによって前記第１更新時点を示すために使用される、項目１２に記載の方法。

（項目１４）

前記第１目標鍵は、前記第１更新時点から開始する前記第１目標鍵の前記有効期間内に適用される、項目１２に記載の方法。

（項目１５）

前記第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、前記第１応答メッセージは第２鍵ネゴシエーションアルゴリズムパラメータを更に含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、前記第１鍵ネゴシエーションアルゴリズムパラメータおよび前記第２鍵ネゴシエーションアルゴリズムパラメータに基づいて前記第１目標鍵を生成する段階を含む、項目１１から１４のいずれか一項に記載の方法。

（項目１６）

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、第２目標鍵および前記新規パラメータに基づいて前記第１目標鍵を生成する段階を含む、項目１１から１４のい

ずれか一項に記載の方法。
（項目１７）
前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定する前記段階は、第２目標鍵、前記新規パラメータおよびアルゴリズム識別子に基づいて、前記第１目標鍵を生成する段階であって、前記アルゴリズム識別子は、前記暗号化鍵または前記完全性保護鍵を決定するために使用されるアルゴリズムを識別するために使用される、段階を含む、項目１１から１４のいずれか一項に記載の方法。
（項目１８）
前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つは、前記第２目標鍵に基づいて決定された前記暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、前記第２目標鍵に基づいて決定された前記完全性保護鍵を使用することによって、前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つに対して実行される、項目１１から１７のいずれか一項に記載の方法。
（項目１９）
装置であって、
第１鍵更新要求を第２ノードへ送信するよう構成される送信ユニットであって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含み、前記第１アイデンティティ認証情報は、第１共有鍵を使用することによって生成される、送信ユニットと、
第１応答メッセージを前記第２ノードから受信するよう構成される受信ユニットであって、前記第１応答メッセージは第２アイデンティティ認証情報を含む、受信ユニットと、
前記第１共有鍵を使用することによって、前記第２アイデンティティ認証情報に対する検証を実行するよう構成される検証ユニットと、
前記第２アイデンティティ認証情報に対する前記検証が成功した場合、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するよう構成される決定ユニットと
を備える装置。
（項目２０）
前記第１鍵更新要求は、第１更新時点および前記第１目標鍵の有効期間の少なくとも１つを示すために使用される、項目１９に記載の装置。
（項目２１）
前記第１鍵更新要求は第１フレーム番号または第１媒体アクセス制御ＭＡＣシリアル番号を含み、前記第１鍵更新要求は、前記第１フレーム番号または前記第１ＭＡＣシリアル番号を使用することによって前記第１更新時点を示すために使用される、項目１９に記載の装置。
（項目２２）
前記第１目標鍵は、前記第１更新時点から開始する前記第１目標鍵の前記有効期間内に適用される、項目２０に記載の装置。
（項目２３）
前記第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、前記第１応答メッセージは更に第２鍵ネゴシエーションアルゴリズムパラメータを含み、前記決定ユニットは、前記第１鍵ネゴシエーションアルゴリズムパラメータおよび前記第２鍵ネゴシエーションアルゴリズムパラメータに基づいて前記第１目標鍵を生成するよう構成される、項目１９から２２のいずれか一項に記載の装置。
（項目２４）
前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記決定ユニットは、第２目標鍵および前記新規パラメータに基づいて前記第１目標鍵を生成するよう構成される、項目１９から２２のいずれか一項に記載の装置。
（項目２５）
前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記決定ユニットは

、第２目標鍵、前記新規パラメータおよびアルゴリズム識別子に基づいて前記第１目標鍵を生成するよう構成され、前記アルゴリズム識別子は、暗号化鍵または完全性保護鍵を決定するために使用されるアルゴリズムをマークするために使用される、項目１９から２２のいずれか一項に記載の装置。

（項目２６）

前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つは、前記第２目標鍵に基づいて決定された前記暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、前記第２目標鍵に基づいて決定された前記完全性保護鍵を使用することによって、前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つに対して実行される、項目１９から２５のいずれか一項に記載の装置。

（項目２７）

前記第１鍵更新要求は前記第１フレーム番号を含み、前記第１フレーム番号は、前記第１目標鍵の更新時点を示すために使用され、前記送信ユニットは、第１通信フレームを使用することによって、前記第１鍵更新要求を前記第２ノードへ送信するよう構成され、前記第１通信フレームの第２フレーム番号は、前回の鍵更新中に使用された鍵更新要求に保持される第３フレーム番号より小さく、前記第３フレーム番号は、前回更新された鍵の開始時点を示すために使用され、前記第１フレーム番号は、前記第２フレーム番号より大きく、前記第３フレーム番号より小さい、項目１９から２６のいずれか一項に記載の装置。

（項目２８）

前記通信フレームは、シグナリングプレーンアップリンクフレーム、シグナリングプレーンダウンリンクフレーム、ユーザプレーンアップリンクフレーム、またはユーザプレーンダウンリンクフレームの少なくとも１つを含む、項目２７に記載の装置。

（項目２９）

装置であって、

第１鍵更新要求を第１ノードから受信するよう構成される受信ユニットであって、前記第１鍵更新要求は第１鍵ネゴシエーションパラメータおよび第１アイデンティティ認証情報を含む、受信ユニットと、

第１共有鍵を使用することによって前記第１アイデンティティ認証情報に対する検証を実行するよう構成される検証ユニットと、

前記第１アイデンティティ認証情報に対する前記検証が成功した場合、前記第１鍵ネゴシエーションパラメータに基づいて第１目標鍵を決定するよう構成される決定ユニットと、

第１応答メッセージを前記第１ノードへ送信するよう構成される送信ユニットであって、前記第１応答メッセージは第２アイデンティティ認証情報を含み、前記第２アイデンティティ認証情報は、前記第１共有鍵を使用することによって生成される、送信ユニットと

を備える装置。

（項目３０）

前記第１鍵更新要求は、第１更新時点および前記第１目標鍵の有効期間の少なくとも１つを示すために使用される、項目２９に記載の装置。

（項目３１）

前記第１鍵更新要求は第１フレーム番号または第１媒体アクセス制御ＭＡＣシリアル番号を含み、前記第１鍵更新要求は、前記第１フレーム番号または前記第１ＭＡＣシリアル番号を使用することによって前記第１更新時点を示すために使用される、項目３０に記載の装置。

（項目３２）

前記第１目標鍵は、前記第１更新時点から開始する前記第１目標鍵の前記有効期間内に適用される、項目３０に記載の装置。

（項目３３）

前記第１鍵ネゴシエーションパラメータは第１鍵ネゴシエーションアルゴリズムパラメータを含み、前記第１応答メッセージは第２鍵ネゴシエーションアルゴリズムパラメータ

を含み、前記決定ユニットは、前記第１鍵ネゴシエーションアルゴリズムパラメータおよび前記第２鍵ネゴシエーションアルゴリズムパラメータに基づいて前記第１目標鍵を生成するよう構成される、項目３０から３２のいずれか一項に記載の装置。

（項目３４）

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記決定ユニットは、第２目標鍵および前記新規パラメータに基づいて前記第１目標鍵を生成するよう構成される、項目３０から３２のいずれか一項に記載の装置。

（項目３５）

前記第１鍵ネゴシエーションパラメータは新規パラメータを含み、前記決定ユニットは、第２目標鍵、前記新規パラメータおよびアルゴリズム識別子に基づいて前記第１目標鍵を生成するよう構成され、前記アルゴリズム識別子は、前記暗号化鍵または前記完全性保護鍵を決定するために使用されるアルゴリズムを識別するために使用される、項目３０から３２のいずれか一項に記載の装置。

（項目３６）

前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つは、前記第２目標鍵に基づいて決定された前記暗号化鍵を使用することによって暗号化され、および／または、完全性保護は、前記第２目標鍵に基づいて決定された前記完全性保護鍵を使用することによって、前記第１鍵更新要求および前記第１応答メッセージの少なくとも１つに対して実行される、項目３０から３２のいずれか一項に記載の装置。

（項目３７）

少なくとも１つのプロセッサおよび通信インタフェースを備える装置であって、前記少なくとも１つのプロセッサは、少なくとも１つのメモリに記憶されたコンピュータプログラムを呼び出すよう構成され、項目１から１０のいずれか一項に記載の方法を前記装置が実装することを可能にする、装置。

（項目３８）

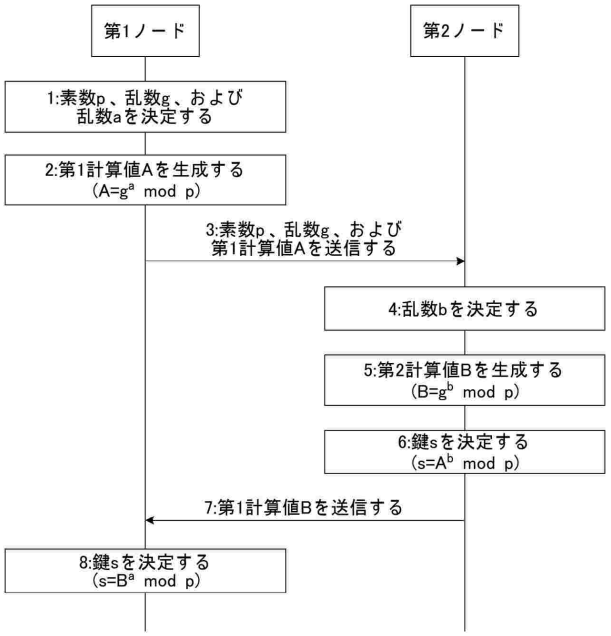
少なくとも１つのプロセッサおよび通信インタフェースを備える装置であって、前記少なくとも１つのプロセッサは、少なくとも１つのメモリに記憶されたコンピュータプログラムを呼び出すよう構成され、項目１１から１８のいずれか一項に記載の方法を前記装置が実装することを可能にする、装置。

（項目３９）

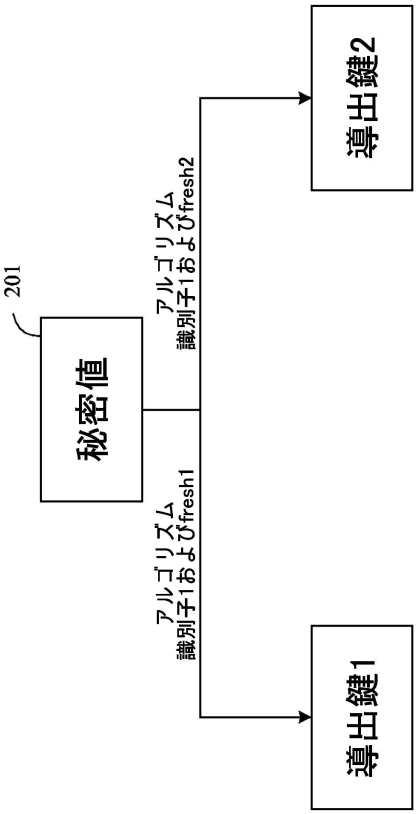
コンピュータプログラムを記憶するコンピュータ可読記憶媒体であって、前記コンピュータプログラムが１または複数のプロセッサ上で実行されるとき、項目１から１８のいずれか一項に記載の方法が実行される、コンピュータ可読記憶媒体。

【図面】

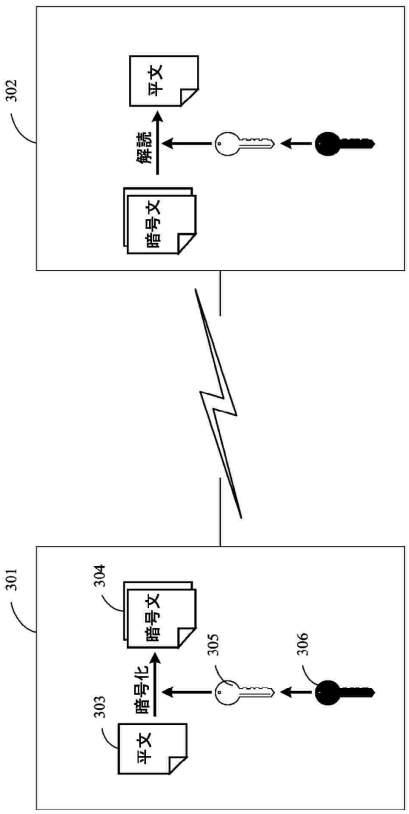
【図１】


第1ノード
第2ノード
1:素数p、乱数g、および
乱数aを決定する
2:第1計算値Aを生成する
(A=g^a mod p)
3:素数p、乱数g、および
第1計算値Aを送信する
4:乱数bを決定する
5:第2計算値Bを生成する
(B=g^b mod p)
6:鍵sを決定する
(s=A^b mod p)
7:第1計算値Bを送信する
8:鍵sを決定する
(s=B^a mod p)

【図２】


201
秘密値
アルゴリズム
識別子1およびfresh2
アルゴリズム
識別子1およびfresh1
導出鍵2
導出鍵1

【図３】



【図４】

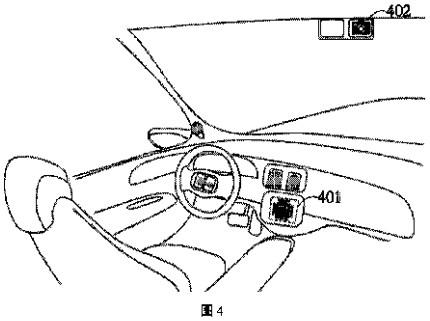
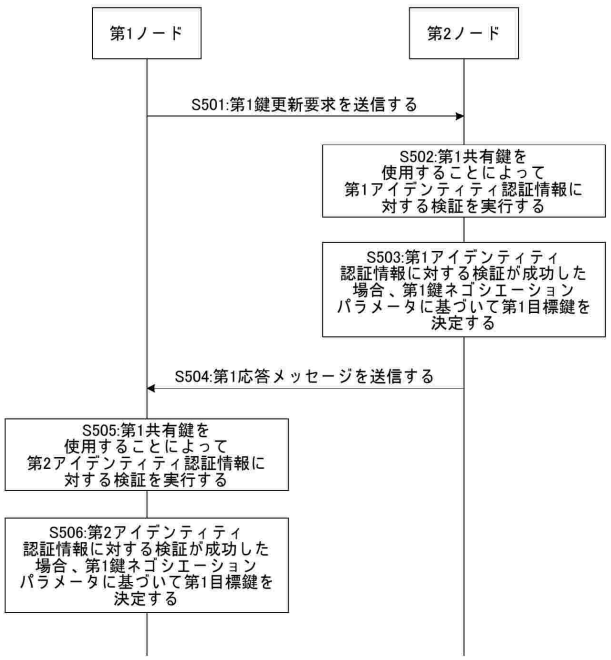
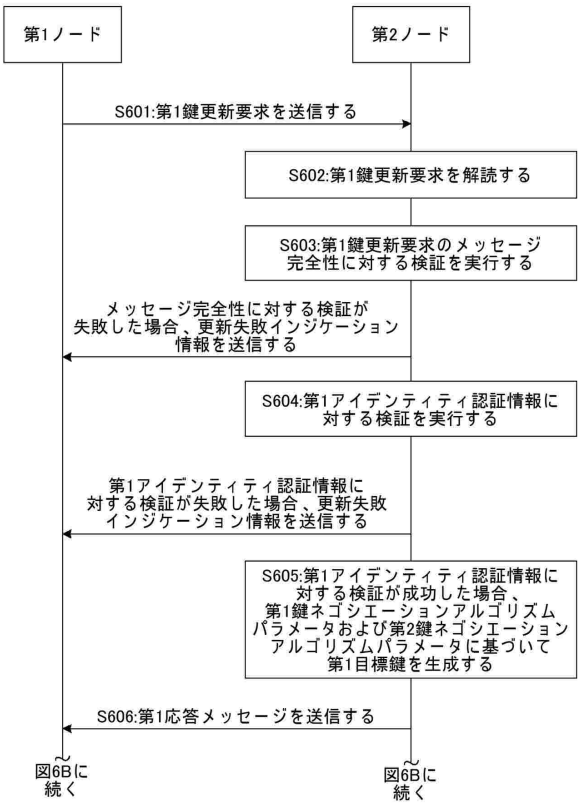


図4

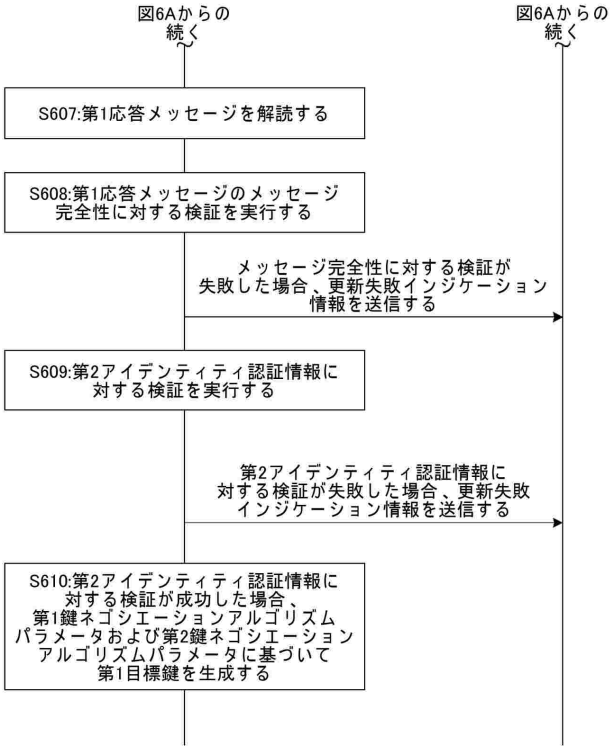
【図５】



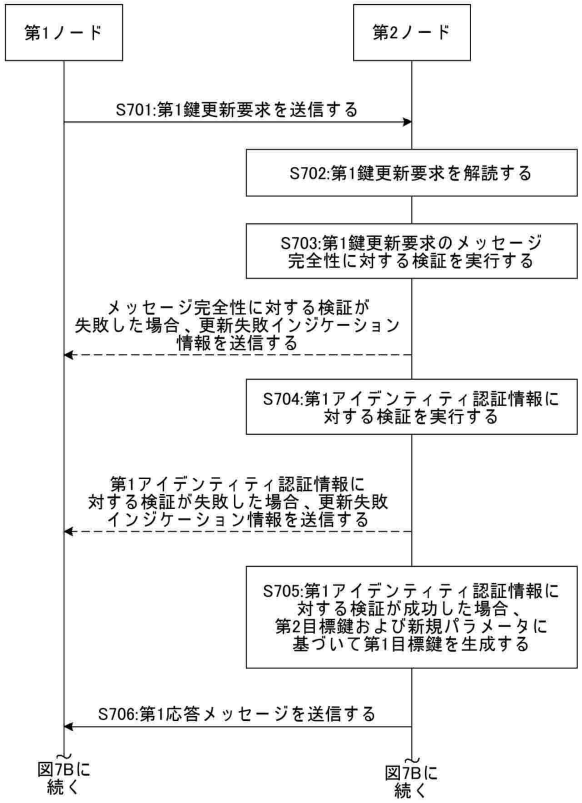
【図６Ａ】



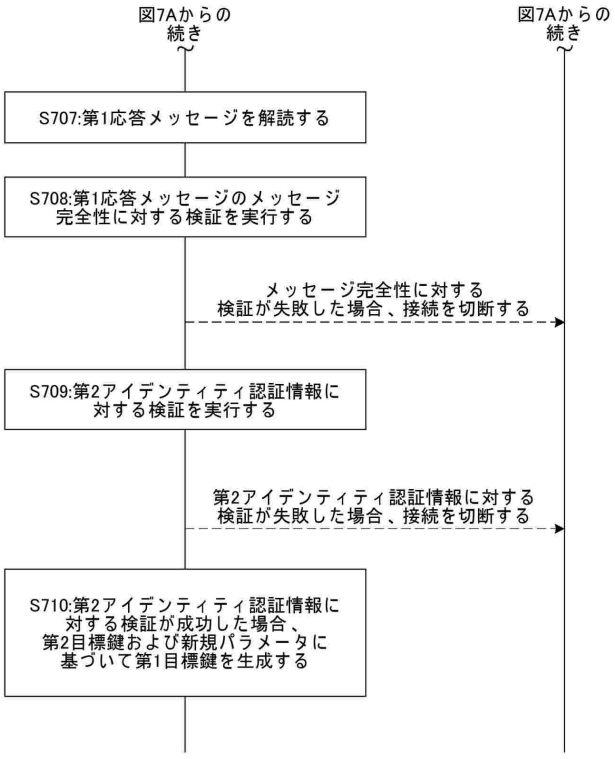
【図６Ｂ】



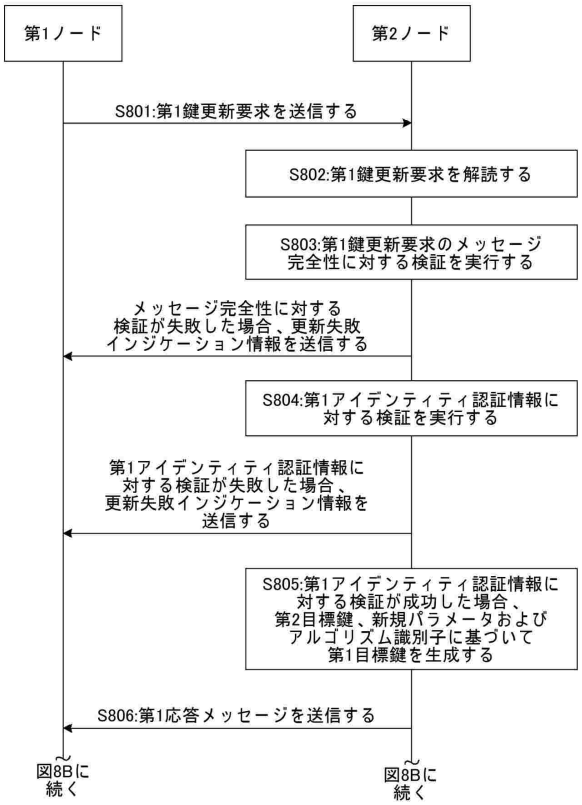
【図７Ａ】



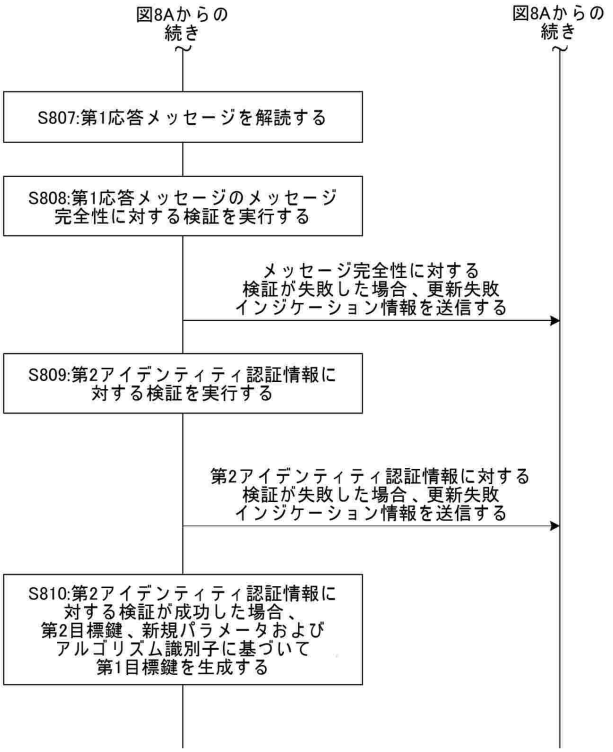
【図７Ｂ】



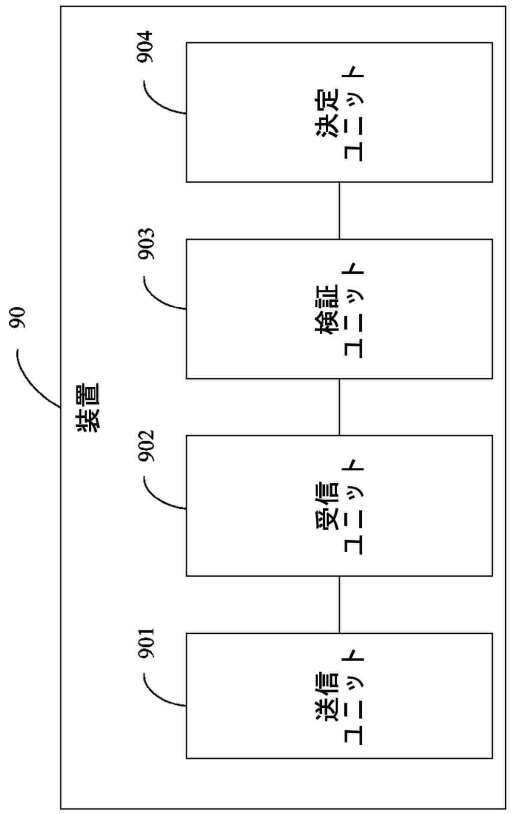
【図８Ａ】



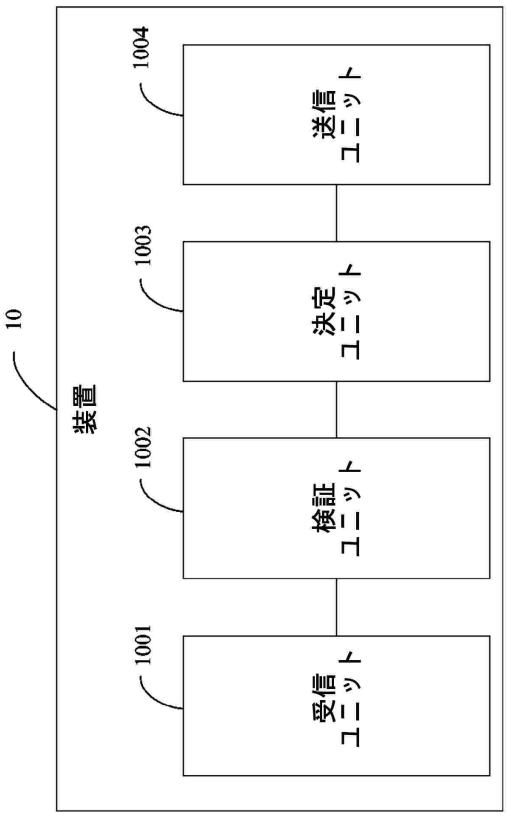
【図８Ｂ】



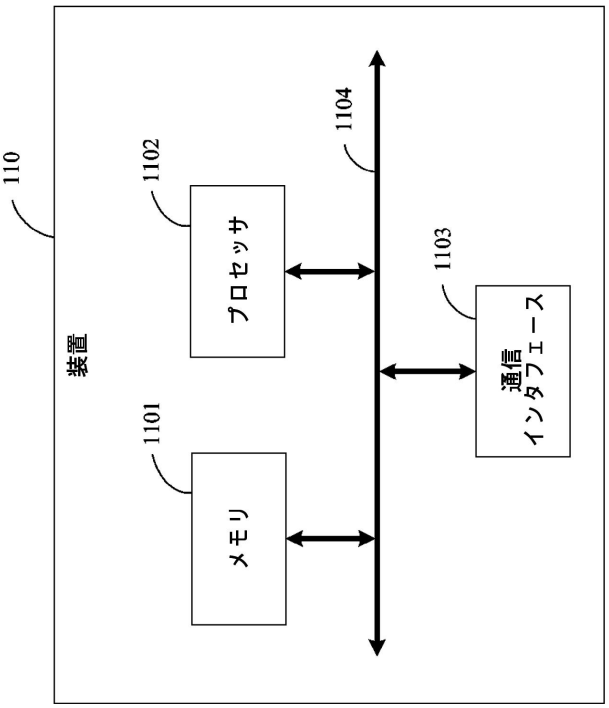
【図９】



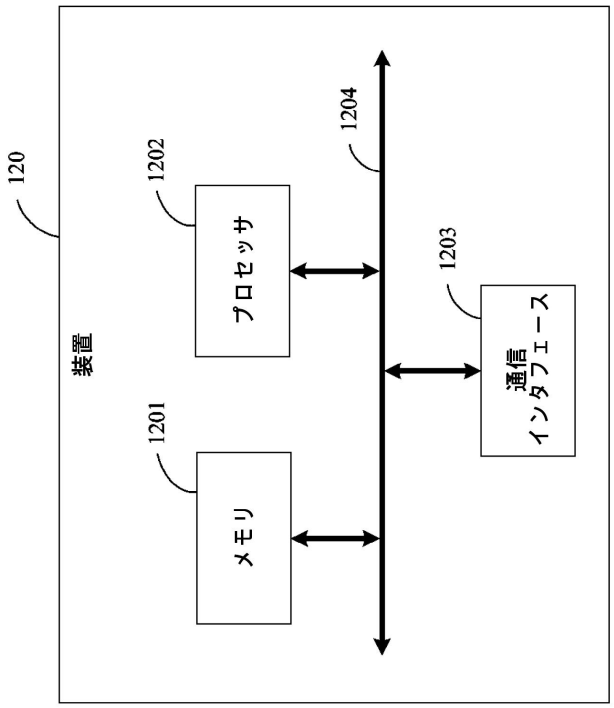
【図１０】



【図１１】



【図１２】



【外国語明細書】
2024081663000017.pdf

フロントページの続き

・ビルディング ホアウェイ・テクノロジーズ・カンパニー・リミテッド内
(72)発明者 チェン、ジン
中華人民共和国・５１８１２９・グァンドン・シェンツェン・ロンガン・ディストリクト・バンティアン・（番地なし）・ホアウェイ・アドミニストレーション・ビルディング ホアウェイ・テクノロジーズ・カンパニー・リミテッド内