

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7521011号
(P7521011)

(45)発行日 令和6年7月23日(2024.7.23)

(24)登録日 令和6年7月12日(2024.7.12)

(51)国際特許分類

F I

H O 4 W 12/10 (2021.01)

H O 4 W 12/03 (2021.01)

H O 4 W 12/041 (2021.01)

H O 4 W 12/10

H O 4 W 12/03

H O 4 W 12/041

請求項の数 45 (全61頁)

(21)出願番号	特願2022-573160(P2022-573160)	(73)特許権者	503433420
(86)(22)出願日	令和2年5月29日(2020.5.29)		華為技術有限公司
(65)公表番号	特表2023-527845(P2023-527845 A)		HUAWEI TECHNOLOGIES CO., LTD.
(43)公表日	令和5年6月30日(2023.6.30)		中華人民共和国 5 1 8 1 2 9 広東省深
(86)国際出願番号	PCT/CN2020/093542		▲チェン▼市龍崗区坂田 華為總部▲ベ
(87)国際公開番号	WO2021/237753		ン▼公樓
(87)国際公開日	令和3年12月2日(2021.12.2)		Huawei Administrat
審査請求日	令和5年1月4日(2023.1.4)		ion Building, Banti
			an, Longgang Distri
			ct, Shenzhen, Guang
			dong 5 1 8 1 2 9, P. R. C
			hina
		(74)代理人	100107766
			弁理士 伊東 忠重

最終頁に続く

(54)【発明の名称】 通信方法及び装置

(57)【特許請求の範囲】

【請求項1】

通信方法であって、当該方法は、

第1アルゴリズムネゴシエーション要求情報を第2ノードから受信するステップであって、前記第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上の鍵導出関数KDFを示すために使用される、ステップと、

前記1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、前記1つ以上のKDFにおける少なくとも1つの第1KDFを決定するステップと、

第1情報を前記第2ノードに送信するステップであって、前記第1情報は、前記少なくとも1つの第1アルゴリズム及び前記少なくとも1つの第1KDFを示すために使用される、ステップと、

を含み、

前記第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを含み、前記第2フレッシュパラメータは、第1ナンスを含み、当該方法は、

第2検証情報を前記第2ノードから受信するステップであって、前記第2検証情報は、前記第1情報、プリセット共有鍵、前記第2フレッシュパラメータ及び前記第1KDFに基づいて取得される、ステップと、

前記第2検証情報を検証するステップと、

を更に含む、方法。

【請求項2】

前記 1 つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む、

請求項 1 に記載の方法。

【請求項 3】

前記少なくとも 1 つの第 1 アルゴリズムを使用することによって、前記第 1 情報に対して完全性保護が実行される、

請求項 2 に記載の方法。

【請求項 4】

前記第 1 情報は、第 2 情報及び第 1 メッセージ認証コード M A C を含み、

前記第 2 情報は、前記少なくとも 1 つの第 1 アルゴリズム及び前記少なくとも 1 つの第 1 K D F を示すために使用され、前記第 1 M A C は、前記第 2 情報に対して完全性保護を実行することによって取得される、

請求項 2 又は 3 に記載の方法。

【請求項 5】

前記少なくとも 1 つの第 1 アルゴリズムは、完全性保護アルゴリズムを含み、前記第 1 M A C は、前記完全性保護アルゴリズムを使用することによって、前記第 2 情報に対して完全性保護を実行することにより取得されるか、又は

前記少なくとも 1 つの第 1 アルゴリズムは、認証された暗号化アルゴリズムを含み、前記第 1 M A C は、前記認証された暗号化アルゴリズムを使用することによって、前記第 2 情報に対して完全性保護を実行することにより取得される、

請求項 4 に記載の方法。

【請求項 6】

前記第 2 情報は、第 1 フレッシュパラメータ及び第 1 検証情報を更に含み、前記第 1 フレッシュパラメータは、前記第 1 情報の時間妥当性に関連するパラメータであり、前記第 1 検証情報は、前記第 1 アルゴリズムネゴシエーション要求情報、プリセット共有鍵、前記第 1 フレッシュパラメータ及び前記第 1 K D F に基づいて取得される、

請求項 4 又は 5 に記載の方法。

【請求項 7】

前記第 1 情報は、暗号化された情報、第 2 通信情報及び第 2 メッセージ認証コード M A C を含み、

前記暗号化された情報は、第 1 通信情報を暗号化することによって取得され、前記第 1 通信情報は、前記少なくとも 1 つの第 1 アルゴリズム又は前記少なくとも 1 つの第 1 K D F のうちの少なくとも一方を示さず、前記第 2 通信情報は、前記少なくとも 1 つの第 1 アルゴリズム又は前記少なくとも 1 つの第 1 K D F のうちの少なくとも一方を示すために使用され、

前記第 2 M A C は、前記暗号化された情報及び前記第 2 通信情報に対して完全性保護を実行することによって取得される、

請求項 2 又は 3 に記載の方法。

【請求項 8】

前記少なくとも 1 つの第 1 アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み、

前記暗号化された情報は、前記暗号化アルゴリズムを使用することによって、前記第 1 通信情報を暗号化することにより取得され、

前記第 2 M A C は、前記完全性保護アルゴリズムを使用することによって、前記暗号化された情報及び前記第 2 通信情報に対して完全性保護を実行することにより取得される、

請求項 7 に記載の方法。

【請求項 9】

前記少なくとも 1 つの第 1 アルゴリズムは、認証された暗号化アルゴリズムを含み、

前記暗号化された情報は、前記認証された暗号化アルゴリズムを使用することによって、前記第 1 通信情報を暗号化することにより取得され、

10

20

30

40

50

前記第 2 MAC は、前記認証された暗号化アルゴリズムを使用することによって、前記暗号化された情報及び前記第 2 通信情報に対して完全性保護を実行することにより取得される、

請求項 7 に記載の方法。

【請求項 10】

前記少なくとも 1 つの第 1 アルゴリズムは、第 1 ノードによってサポートされ、かつ前記 1 つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、前記少なくとも 1 つの第 1 KDF は、前記第 1 ノードによってサポートされ、かつ前記 1 つ以上の KDF において最も高い優先度を有する KDF である、

請求項 1 乃至 9 のいずれか一項に記載の方法。

10

【請求項 11】

当該方法は、

第 2 アルゴリズムネゴシエーション要求情報を前記第 2 ノードから受信するステップであって、前記第 2 アルゴリズムネゴシエーション要求情報は、1 つ以上のアルゴリズム及び 1 つ以上の KDF を示すために使用される、ステップと、

第 3 情報を前記第 2 ノードに送信するステップであって、前記第 3 情報は、前記第 2 アルゴリズムネゴシエーション要求情報によって示される前記 1 つ以上のアルゴリズム及び前記 1 つ以上の KDF がサポートされていないか又は適用可能でないことを示すために使用される、ステップと、

を更に含む、請求項 1 乃至 10 のいずれか一項に記載の方法。

20

【請求項 12】

前記第 2 アルゴリズムネゴシエーション要求情報によって示される前記 1 つ以上のアルゴリズムは、前記第 1 アルゴリズムネゴシエーション要求情報によって示される前記 1 つ以上のアルゴリズムとは異なり、

前記第 2 アルゴリズムネゴシエーション要求情報によって示される前記 1 つ以上の KDF は、前記第 1 アルゴリズムネゴシエーション要求情報によって示される前記 1 つ以上の KDF とは異なる、

請求項 11 に記載の方法。

【請求項 13】

通信方法であって、当該方法は、

30

第 1 アルゴリズムネゴシエーション要求情報を第 1 ノードに送信するステップであって、前記第 1 アルゴリズムネゴシエーション要求情報は、1 つ以上のアルゴリズム及び 1 つ以上の鍵導出関数 KDF を示すために使用される、ステップと、

第 1 情報を前記第 1 ノードから受信するステップであって、前記第 1 情報は、前記 1 つ以上のアルゴリズムにおける少なくとも 1 つの第 1 アルゴリズムと、前記 1 つ以上の KDF における少なくとも 1 つの第 1 KDF を示すために使用される、ステップと、

を含み、

前記第 1 アルゴリズムネゴシエーション要求情報は、第 2 フレッシュパラメータを更に含み、前記第 2 フレッシュパラメータは、第 1 ナンスを含み、当該方法は、

第 2 検証情報を前記第 1 ノードに送信するステップであって、前記第 2 検証情報は、前記第 1 情報、プリセット共有鍵、前記第 2 フレッシュパラメータ及び前記第 1 KDF に基づいて取得される、ステップ、

40

を更に含む、方法。

【請求項 14】

前記 1 つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む、

請求項 13 に記載の方法。

【請求項 15】

前記少なくとも 1 つの第 1 アルゴリズムを使用することによって、前記第 1 情報に対して完全性保護が実行される、

50

請求項 14 に記載の方法。

【請求項 16】

前記第 1 情報は、第 2 情報及び第 1 メッセージ認証コード MAC を含み、

前記第 2 情報は、前記少なくとも 1 つの第 1 アルゴリズム及び前記少なくとも 1 つの第 1 KDF を示すために使用され、前記第 1 MAC は、前記第 2 情報に対して完全性保護を実行することによって取得される、

請求項 14 又は 15 に記載の方法。

【請求項 17】

前記少なくとも 1 つの第 1 アルゴリズムは、完全性保護アルゴリズムを含み、前記第 1 MAC は、前記完全性保護アルゴリズムを使用することによって、前記第 2 情報に対して完全性保護を実行することにより取得され、当該方法は、前記完全性保護アルゴリズム及び前記第 2 情報に基づいて第 3 MAC を取得するステップを更に含み、前記第 3 MAC は、前記第 2 情報の完全性を検証するために使用されるか、又は

前記少なくとも 1 つの第 1 アルゴリズムは、認証された暗号化アルゴリズムを含み、前記第 1 MAC は、前記認証された暗号化アルゴリズムを使用することによって、前記第 2 情報に対して完全性保護を実行することにより取得され、当該方法は、前記認証された暗号化アルゴリズム及び前記第 2 情報に基づいて第 3 MAC を取得するステップを更に含み、前記第 3 MAC は、前記第 2 情報の完全性を検証するために使用される、

請求項 16 に記載の方法。

【請求項 18】

前記第 2 情報は、第 1 フレッシュパラメータ及び第 1 検証情報を更に含み、前記第 1 フレッシュパラメータは、前記第 1 情報の時間妥当性に関連するパラメータであり、前記第 1 検証情報は、前記第 1 アルゴリズムネゴシエーション要求情報、プリセット共有鍵、前記第 1 フレッシュパラメータ及び前記第 1 KDF に基づいて取得される、

請求項 16 又は 17 に記載の方法。

【請求項 19】

前記第 1 情報は、暗号化された情報、第 2 通信情報及び第 2 メッセージ認証コード MAC を含み、

前記暗号化された情報は、第 1 通信情報を暗号化することによって取得され、前記第 1 通信情報は、前記少なくとも 1 つの第 1 アルゴリズム又は前記少なくとも 1 つの第 1 KDF のうちの少なくとも一方を示さず、前記第 2 通信情報は、前記少なくとも 1 つの第 1 アルゴリズム又は前記少なくとも 1 つの第 1 KDF のうちの少なくとも一方を示すために使用され、

前記第 2 MAC は、前記暗号化された情報及び前記第 2 通信情報に対して完全性保護を実行することによって取得される、

請求項 14 又は 15 に記載の方法。

【請求項 20】

前記少なくとも 1 つの第 1 アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み、

前記暗号化された情報は、前記暗号化アルゴリズムを使用することによって、前記第 1 通信情報を暗号化することにより取得され、

前記第 2 MAC は、前記完全性保護アルゴリズムを使用することによって、前記暗号化された情報及び前記第 2 通信情報に対して完全性保護を実行することにより取得され、

当該方法は、

前記完全性保護アルゴリズム、前記暗号化された情報及び前記第 2 通信情報に基づいて第 4 MAC を取得するステップと、

前記第 4 MAC が前記第 2 MAC と同じである場合、前記暗号化アルゴリズムを使用することによって、前記暗号化された情報を復号するステップと、

を更に含む、請求項 19 に記載の方法。

【請求項 21】

前記少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、
前記暗号化された情報は、前記認証された暗号化アルゴリズムを使用することによって、
前記第1通信情報を暗号化することにより取得され、

前記第2MACは、前記認証された暗号化アルゴリズムを使用することによって、前記暗号化された情報及び前記第2通信情報に対して完全性保護を実行することにより取得され、

当該方法は、

前記認証された暗号化アルゴリズム、前記暗号化された情報及び前記第2通信情報に基づいて第4MACを取得するステップと、

前記第4MACが前記第2MACと同じである場合、前記認証された暗号化アルゴリズムを使用することによって、前記暗号化された情報を復号するステップと、

を更に含む、請求項19に記載の方法。

【請求項22】

前記少なくとも1つの第1アルゴリズムは、前記第1ノードによってサポートされ、かつ前記1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、前記少なくとも1つの第1KDFは、前記第1ノードによってサポートされ、かつ前記1つ以上のKDFにおいて最も高い優先度を有するKDFである、

請求項13乃至21のいずれか一項に記載の方法。

【請求項23】

当該方法は、

第2アルゴリズムネゴシエーション要求情報を前記第1ノードに送信するステップであって、前記第2アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される、ステップと、

第3情報を前記第1ノードから受信するステップであって、前記第3情報は、前記第2アルゴリズムネゴシエーション要求情報によって示される前記1つ以上のアルゴリズム及び前記1つ以上のKDFがサポートされていないか又は適用可能でないことを示すために使用される、ステップと、

を更に含む、請求項13乃至22のいずれか一項に記載の方法。

【請求項24】

前記第2アルゴリズムネゴシエーション要求情報によって示される前記1つ以上のアルゴリズムは、前記第1アルゴリズムネゴシエーション要求情報によって示される前記1つ以上のアルゴリズムとは異なり、

前記第2アルゴリズムネゴシエーション要求情報によって示される前記1つ以上のKDFは、前記第1アルゴリズムネゴシエーション要求情報によって示される前記1つ以上のKDFとは異なる、

請求項23に記載の方法。

【請求項25】

通信装置であって、当該通信装置は、受信モジュールと、処理モジュールと、送信モジュールとを含み、

前記受信モジュールは、第1アルゴリズムネゴシエーション要求情報を第2ノードから受信するよう構成され、前記第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上の鍵導出関数KDFを示すために使用され、

前記処理モジュールは、前記1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、前記1つ以上のKDFにおける少なくとも1つの第1KDFを決定するよう構成され、

前記送信モジュールは、第1情報を前記第2ノードに送信するよう構成され、前記第1情報は、前記少なくとも1つの第1アルゴリズム及び前記少なくとも1つの第1KDFを示すために使用され、

前記第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを更に含み、前記第2フレッシュパラメータは、第1ナンスを含み、

10

20

30

40

50

前記受信モジュールは、第2検証情報を前記第2ノードから受信するよう更に構成され、前記第2検証情報は、前記第1情報、プリセット共有鍵、前記第2フレッシュパラメータ及び前記第1KDFに基づいて取得され、

前記処理モジュールは、前記第2検証情報を検証するよう更に構成される、通信装置。

【請求項26】

前記1つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む、

請求項25に記載の通信装置。

【請求項27】

前記少なくとも1つの第1アルゴリズムを使用することによって、前記第1情報に対して完全性保護が実行される、

請求項26に記載の通信装置。

【請求項28】

前記第1情報は、第2情報及び第1メッセージ認証コードMACを含み、

前記第2情報は、前記少なくとも1つの第1アルゴリズム及び前記少なくとも1つの第1KDFを示すために使用され、前記第1MACは、前記第2情報に対して完全性保護を実行することによって取得される、

請求項26又は27に記載の通信装置。

【請求項29】

前記少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズムを含み、前記第1MACは、前記完全性保護アルゴリズムを使用することによって、前記第2情報に対して完全性保護を実行することにより取得されるか、又は

前記少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、前記第1MACは、前記認証された暗号化アルゴリズムを使用することによって、前記第2情報に対して完全性保護を実行することにより取得される、

請求項28に記載の通信装置。

【請求項30】

前記第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含み、前記第1フレッシュパラメータは、前記第1情報の時間妥当性に関連するパラメータであり、前記第1検証情報は、前記第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵、前記第1フレッシュパラメータ及び前記第1KDFに基づいて取得される、

請求項28又は29に記載の通信装置。

【請求項31】

前記少なくとも1つの第1アルゴリズムは、当該通信装置によってサポートされ、かつ前記1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、前記少なくとも1つの第1KDFは、当該通信装置によってサポートされ、かつ前記1つ以上のKDFにおいて最も高い優先度を有するKDFである、

請求項25乃至30のいずれか一項に記載の通信装置。

【請求項32】

通信装置であって、当該通信装置は、送信モジュールと、受信モジュールとを含み、

前記送信モジュールは、第1アルゴリズムネゴシエーション要求情報を第1ノードに送信するよう構成され、前記第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上の鍵導出関数KDFを示すために使用され、

前記受信モジュールは、第1情報を前記第1ノードから受信するよう構成され、前記第1情報は、前記1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、前記1つ以上のKDFにおける少なくとも1つの第1KDFを示すために使用され、

前記第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを更に含み、前記第2フレッシュパラメータは、第1ナンスを含み、

前記送信モジュールは、第2検証情報を前記第1ノードに送信するよう更に構成され、

10

20

30

40

50

前記第 2 検証情報は、前記第 1 情報、プリセット共有鍵、前記第 2 フレッシュパラメータ及び前記第 1 K D F に基づいて取得される、

通信装置。

【請求項 3 3】

前記 1 つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む、

請求項 3 2 に記載の通信装置。

【請求項 3 4】

前記少なくとも 1 つの第 1 アルゴリズムを使用することによって、前記第 1 情報に対して完全性保護が実行される、

請求項 3 3 に記載の通信装置。

【請求項 3 5】

前記第 1 情報は、第 2 情報及び第 1 メッセージ認証コード M A C を含み、

前記第 2 情報は、前記少なくとも 1 つの第 1 アルゴリズム及び前記少なくとも 1 つの第 1 K D F を示すために使用され、前記第 1 M A C は、前記第 2 情報に対して完全性保護を実行することによって取得される、

請求項 3 3 又は 3 4 に記載の通信装置。

【請求項 3 6】

当該通信装置は、処理モジュールを更に含み、

前記少なくとも 1 つの第 1 アルゴリズムは、完全性保護アルゴリズムを含み、前記第 1 M A C は、前記完全性保護アルゴリズムを使用することによって、前記第 2 情報に対して完全性保護を実行することにより取得され、前記処理モジュールは、前記完全性保護アルゴリズム及び前記第 2 情報に基づいて第 3 M A C を取得するよう構成され、前記第 3 M A C は、前記第 2 情報の完全性を検証するために使用されるか、又は

前記少なくとも 1 つの第 1 アルゴリズムは、認証された暗号化アルゴリズムを含み、前記第 1 M A C は、前記認証された暗号化アルゴリズムを使用することによって、前記第 2 情報に対して完全性保護を実行することにより取得され、前記処理モジュールは、前記認証された暗号化アルゴリズム及び前記第 2 情報に基づいて第 3 M A C を取得するよう構成され、前記第 3 M A C は、前記第 2 情報の完全性を検証するために使用される、

請求項 3 5 に記載の通信装置。

【請求項 3 7】

前記第 2 情報は、第 1 フレッシュパラメータ及び第 1 検証情報を更に含み、前記第 1 フレッシュパラメータは、前記第 1 情報の時間妥当性に関連するパラメータであり、前記第 1 検証情報は、前記第 1 アルゴリズムネゴシエーション要求情報、プリセット共有鍵、前記第 1 フレッシュパラメータ及び前記第 1 K D F に基づいて取得される、

請求項 3 5 又は 3 6 に記載の通信装置。

【請求項 3 8】

前記少なくとも 1 つの第 1 アルゴリズムは、前記第 1 ノードによってサポートされ、かつ前記 1 つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、前記少なくとも 1 つの第 1 K D F は、前記第 1 ノードによってサポートされ、かつ前記 1 つ以上の K D F において最も高い優先度を有する K D F である、

請求項 3 2 乃至 3 7 のいずれか一項に記載の通信装置。

【請求項 3 9】

少なくとも 1 つのプロセッサを含む通信装置であって、前記少なくとも 1 つのプロセッサは、メモリに結合され、前記メモリは、プログラム又は命令を記憶するよう構成され、前記プログラム又は前記命令が前記プロセッサによって実行されると、当該装置は、請求項 1 乃至 1 2 のいずれか一項に記載の方法を実行することができる、通信装置。

【請求項 4 0】

少なくとも 1 つのプロセッサを含む通信装置であって、前記少なくとも 1 つのプロセッサは、メモリに結合され、前記メモリは、プログラム又は命令を記憶するよう構成され、

10

20

30

40

50

前記プログラム又は前記命令が前記プロセッサによって実行されると、当該装置は、請求項 1 3 乃至 2 4 のいずれか一項に記載の方法を実行することができる、通信装置。

【請求項 4 1】

コンピュータ読取可能媒体であって、当該コンピュータ読取可能媒体は、コンピュータプログラム又は命令を記憶し、前記コンピュータプログラム又は前記命令が実行されると、コンピュータは、請求項 1 乃至 1 2 のいずれか一項に記載の方法を実行することができる、コンピュータ読取可能媒体。

【請求項 4 2】

コンピュータ読取可能媒体であって、当該コンピュータ読取可能媒体は、コンピュータプログラム又は命令を記憶し、前記コンピュータプログラム又は前記命令が実行されると、コンピュータは、請求項 1 3 乃至 2 4 のいずれか一項に記載の方法を実行することができる、コンピュータ読取可能媒体。

【請求項 4 3】

請求項 3 9 に記載の装置及び請求項 4 0 に記載の装置を含む通信システム。

【請求項 4 4】

コンピュータに、請求項 1 乃至 1 2 のいずれか一項のステップを実行させるプログラム。

【請求項 4 5】

コンピュータに、請求項 1 3 乃至 2 4 のいずれか一項のステップを実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本出願の実施形態は、無線通信分野に関し、特に、通信方法及び装置に関する。本方法及び装置は、短距離通信分野、例えばコックピットドメインに適用することができ、自動運転又はインテリジェント運転のようなシナリオに適用可能である。

【背景技術】

【0 0 0 2】

データ伝送中、データ伝送の安全性を確保するために、送信者は、アルゴリズムを使用することによってデータを暗号化し、暗号化されたデータを受信者に送信する。暗号化されたデータを受信した後、受信者は、アルゴリズムを使用することによって、暗号化されたデータを復号してデータを取得する。受信者が送信者によって送信されたデータを正しく復号できるようにするために、受信者は、通常の通信を確保するために、送信者と同じアルゴリズムを使用して、暗号化されたデータを復号する必要がある。

【0 0 0 3】

しかしながら、従来の技術では、通信暗号化に関連するアルゴリズムには多くのタイプがある。送信者及び受信者の能力の設定とシナリオの要件に基づいて、送信者及び受信者は多くのタイプのアルゴリズムをサポートする可能性がある。したがって、送信者と受信者が同じアルゴリズムを使用することによりデータに対して暗号化又は復号のような処理を正確かつ効率的に実行することを可能にする方法は、通信効率と性能にとって重要である。

【発明の概要】

【発明が解決しようとする課題】

【0 0 0 4】

本出願の実施形態は、送信者及び受信者が通信情報の暗号化又は復号に関連する処理を正確かつ効率的に実行することができるように、通信方法及び装置を提供する。

【課題を解決するための手段】

【0 0 0 5】

前述の目的を達成するために、以下の技術的解決策が本出願の実施態様において使用される。

【0 0 0 6】

第1の態様によると、本出願の実施形態は、通信方法を提供する。本方法は、第1ノードに適用され、本方法は：第1アルゴリズムネゴシエーション要求情報を第2ノードから受信するステップであって、第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上の鍵導出関数（`key derivation function`、`KDF`）を示すために使用される、ステップと；1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、1つ以上の`KDF`における少なくとも1つの第1`KDF`を決定するステップと；第1情報を第2ノードに送信するステップであって、第1情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1`KDF`を示すために使用される、ステップと；を含む。

【0007】

第1の態様において提供される方法によると、1つ以上のアルゴリズム及び1つ以上の`KDF`を示すために使用される第1アルゴリズムネゴシエーション要求情報を、第2ノードから受信することができ、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1`KDF`を、第1アルゴリズムネゴシエーション要求情報に基づいて決定することができ、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1`KDF`を示すために使用される第1情報を、第2ノードに送信することができる。このようにして、第1ノードは、アルゴリズム及び`KDF`について第2ノードとネゴシエーションすることができ、その結果、第1ノードと第2ノードは、通信情報に対する暗号化又は復号に関連する処理を正確かつ効率的に実行する。第1ノードが第2ノードに情報を送信する例を使用する。第1ノードは、ネゴシエーションされたアルゴリズム及び`KDF`に従って情報を暗号化し、暗号化された情報を第2ノードに送信し得る。暗号化された情報を受信した後、第2ノードは、ネゴシエーションされたアルゴリズムと`KDF`に従って、暗号化された情報を復号し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

【0008】

第1の態様に関連して、ある可能な実装では、1つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む。前述の方法に基づいて、第1ノードと第2ノードは、暗号化アルゴリズム、完全性保護アルゴリズム又は認証された暗号化アルゴリズムのような複数のアルゴリズムを使用することによって、互いに通信し得る。これにより、第1ノードと第2ノードとの間の通信に使用されるアルゴリズムの多様性が改善される。

【0009】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護が実行される。前述の方法に基づいて、第1ノードは、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護を実行し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

【0010】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、第1情報は、第2情報及び第1メッセージ認証コード（`message authentication code`、`MAC`）を含み、第2情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1`KDF`を示すために使用され、第1`MAC`は、第2情報に対して完全性保護を実行することによって取得される。前述の方法に基づいて、第1ノードは、第2情報及び第1`MAC`を第2ノードに送信し、第1`MAC`を使用することによって第2情報の完全性保護を実行し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

【0011】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズムを含み、第1`MAC`は、完全性保護アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することによって取得されるか；又は少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴ

10

20

30

40

50

リズムを含み、第1MACは、認証された暗号化アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得される。前述の方法に基づいて、第1ノードは、複数のアルゴリズムを使用することによって、第2情報に対して完全性保護を実行し得る。これにより、第1ノードと第2ノードとの間の情報に対して第1ノードによって実行される完全性保護の柔軟性と多様性が改善される。

【0012】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含み、第1フレッシュパラメータは、第1情報の時間妥当性に関連するパラメータであり、第1検証情報は、第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵、第1フレッシュパラメータ及び第1KDFに基づいて取得される。前述の方法に基づいて、第1ノードは、第1検証情報に基づいて、第1アルゴリズムネゴシエーション要求情報に対して完全性保護を更に実行し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

10

【0013】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、第1情報は、暗号化された情報、第2通信情報及び第2MACを含み；暗号化された情報は、第1通信情報を暗号化することによって取得され、第1通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示さず、第2通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示すために使用され；第2MACは、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得される。上述の方法に基づいて、第1ノードは、第1通信情報を暗号化して暗号化された情報を取得し、第2MACを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

20

【0014】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み；暗号化された情報は、暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、完全性保護アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することにより取得される。前述の方法に基づいて、第1ノードは更に、暗号化アルゴリズムを使用することによって第1通信情報を暗号化し、完全性保護アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

30

【0015】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み；暗号化された情報は、認証された暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することにより取得される。前述の方法に基づいて、第1ノードは更に、認証された暗号化アルゴリズムを使用することによって第1通信情報を暗号化し、認証された暗号化アルゴリズムを使用することによって暗号化された情報及び第2通信情報に対して完全性保護を実行し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

40

【0016】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、第1ノードによってサポートされ、かつ1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、少なくとも1つの第1KDFは、第1ノードによってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFである。前述の方法に基づいて、アルゴリズムの優先度はアルゴリズムの

50

セキュリティに基づいて取得され、使用されるアルゴリズムの優先度が高いほど通信セキュリティが高いことを示すため、第1ノードは、該第1ノードによってサポートされ、かつ1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムと、該第1ノードによってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFを使用することによって、第2ノードと通信する。これにより、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

【0017】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは1つ以上のアルゴリズムタイプに対応し、少なくとも1つの第1アルゴリズムに対応するアルゴリズムタイプは、第1ノードによってサポートされ、かつ1つ以上のアルゴリズムの1つ以上のアルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムタイプである。前述の方法に基づいて、第1ノードは、該第1ノードと第2ノードの両方によってサポートされるアルゴリズムタイプにおいて、最も高い優先度を有するアルゴリズムタイプを決定することができ、その結果、第1ノードは、最も高い優先度を有するアルゴリズムタイプに対応する少なくとも1つの第1アルゴリズムを決定する。

10

【0018】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは1つのアルゴリズムタイプに対応し、該アルゴリズムタイプは異なる優先度を有する複数のアルゴリズムに対応してよく、第1アルゴリズムは、第1ノードによってサポートされ、かつ上記のアルゴリズムタイプに対応するアルゴリズムにおいて最も高い優先度を有するアルゴリズムである。前述の方法に基づいて、少なくとも1つの第1アルゴリズムが1つのアルゴリズムタイプに対応するとき、第1ノードは、該第1ノードによってサポートされ、かつ第1アルゴリズムに対応するアルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムを、第1アルゴリズムとして決定し得る。あるいは、アルゴリズムタイプが1つのアルゴリズムのみに対応する場合、第1ノードは、第1アルゴリズムが、そのアルゴリズムを含むことを決定する。このようにして、第1ノードは、比較的高い優先度を有するアルゴリズムを使用することによって、第2ノードと通信し得る。通常、アルゴリズムの優先度は、アルゴリズムのセキュリティに関連する。したがって、第1ノードと第2ノードは、比較的高い優先度を有するアルゴリズムを使用することによって互いに通信し、その結果、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

20

30

【0019】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、複数のアルゴリズムタイプに対応し、該複数のアルゴリズムタイプの優先度は同じである。各アルゴリズムタイプは、異なる優先度を有する1つ以上のアルゴリズムに対応してよく、少なくとも1つの第1アルゴリズムは、第1ノードによってサポートされ、かつ複数のアルゴリズムタイプの各々に対応するアルゴリズムにおいて最も高い優先度を有するアルゴリズムを含む。あるいは、アルゴリズムタイプが1つのアルゴリズムのみに対応する場合、少なくとも1つの第1アルゴリズムは、そのアルゴリズムタイプに対応するアルゴリズムを含む。前述の方法に基づいて、少なくとも1つの第1アルゴリズムが複数のアルゴリズムタイプに対応するとき、第1ノードは、該第1ノードによってサポートされ、かつ各アルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムを第1アルゴリズムとして決定し得る。このようにして、第1ノードは、比較的高い優先度を有するアルゴリズムを使用することによって、第2ノードと通信し得る。通常、アルゴリズムの優先度は、アルゴリズムのセキュリティに関連する。したがって、第1ノードと第2ノードは、比較的高い優先度を有するアルゴリズムを使用することによって互いに通信し、その結果、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

40

【0020】

50

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを含み、第2フレッシュパラメータは、第1アルゴリズムネゴシエーション要求情報の時間妥当性に関連するパラメータであり、方法は：第2検証情報を第2ノードから受信するステップであって、第2検証情報は、第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて取得される、ステップと；第1情報、共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて、第2検証情報を検証するステップと；を更に含む。前述の方法に基づいて、第1ノードは、第1情報、共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて、第2ノードによって受信された第1情報が変更されているかどうかを検証することができ、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

10

【0021】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、方法は：第2アルゴリズムネゴシエーション要求情報を第2ノードから受信するステップであって、第2アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される、ステップと；第3情報を第2ノードに送信するステップであって、第3情報は、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFがサポートされていないか又は適用可能でないことを示すために使用される、ステップと；を更に含む。前述の方法に基づいて、第1ノードは、第2ノードからのものであって、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される、第2アルゴリズムネゴシエーション要求情報を受信し、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFがサポートされていないか又は適用可能でないことを示すために使用される第3情報を、第2ノードに送信し得る。このようにして、第1ノードと第2ノードは、通信を複数回行うことによってアルゴリズム及びKDFをネゴシエーションすることができ、第1ノードと第2ノードによるアルゴリズム及びKDFのネゴシエーションの成功率を改善することができる。

20

【0022】

第1の態様及び該第1の態様の可能な実装に関連して、ある可能な実装では、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムとは異なり；第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFとは異なる。前述の方法に基づいて、第1ノードは、第2ノードによって複数回示される1つ以上のアルゴリズム及び1つ以上のKDFを取得することができ、その結果、第1ノードは、1つ以上の取得されたアルゴリズム及び1つ以上の取得されたKDFに基づいて、第2ノードとの通信に使用されるアルゴリズム及びKDFを決定する。これにより、第1ノードと第2ノードによるアルゴリズム及びKDFのネゴシエーションの成功率を改善する。

30

【0023】

第2の態様によると、本出願の実施形態は、通信方法を提供する。本方法は、第2ノードに適用され、本方法は：第1アルゴリズムネゴシエーション要求情報を第1ノードに送信するステップであって、第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される、ステップと；第1情報を第1ノードから受信するステップであって、第1情報は、1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、1つ以上のKDFにおける少なくとも1つの第1KDFを示すために使用される、ステップと；を含む。

40

【0024】

第2の態様において提供される方法によると、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される第1アルゴリズムネゴシエーション要求情報を、第1ノードに送信することができ、1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴ

50

リズム及び1つ以上のKDFにおける少なくとも1つの第1KDFを示すために使用される第1情報を、第2ノードから受信することができる。このようにして、第1ノードと第2ノードはアルゴリズム及びKDFをネゴシエーションし、ネゴシエーションされたアルゴリズムとKDFを使用することによって互いに通信することができ、その結果、第1ノードと第2ノードは、通信情報に対する暗号化又は復号に関連する処理を正確かつ効率的に実行する。

【0025】

第2の態様に関連して、ある可能な実装では、1つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む。前述の方法に基づいて、第1ノードと第2ノードは、暗号化アルゴリズム、完全性保護アルゴリズム又は認証された暗号化アルゴリズムのような複数のアルゴリズムを使用することによって、互いに通信し得る。これにより、第1ノードと第2ノードとの間の通信に使用されるアルゴリズムの多様性が改善される。

10

【0026】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護が実行される。前述の方法に基づいて、第2ノードは、少なくとも1つの第1アルゴリズムを使用することによって、第1情報の完全性を検証し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

【0027】

20

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、第1情報は、第2情報及び第1メッセージ認証コードMACを含み、第2情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを示すために使用され、第1MACは、第2情報に対して完全性保護を実行することによって取得される。前述の方法に基づいて、第2ノードは、第2情報及び第1MACを第1ノードから受信することができ、ここで、第1MACを使用することによって第2情報に対して完全性保護が実行される。これにより、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

【0028】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズムを含み、第1MACは、完全性保護アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得され、方法は、完全性保護アルゴリズム及び第2情報に基づいて第3MACを取得するステップを更に含み、第3MACは、第2情報の完全性を検証するために使用されるか；又は、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、第1MACは、認証された暗号化アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得され、方法は、認証された暗号化アルゴリズム及び第2情報に基づいて第3MACを取得するステップを更に含み、第3MACは、第2情報の完全性を検証するために使用される。前述の方法に基づいて、第2ノードは、複数のアルゴリズムに従って第2情報の完全性を検証し得る。これにより、第2ノードが情報の完全性を検証するとき、第2ノードの柔軟性と多様性を改善する。

30

40

【0029】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含み、第1フレッシュパラメータは、第1情報の時間妥当性に関連するパラメータであり、第1検証情報は、第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵、第1フレッシュパラメータ及び第1KDFに基づいて取得される。前述の方法に基づいて、第2ノードは、第1検証情報を使用することによって、第1アルゴリズムネゴシエーション要求情報の完全性を更に検証し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

【0030】

50

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、第1情報は、暗号化された情報、第2通信情報及び第2MACを含み；暗号化された情報は、第1通信情報を暗号化することによって取得され、第1通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示さず、第2通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示すために使用され；第2MACは、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得される。前述の方法に基づいて、第2ノードは、暗号化された情報、第2通信情報及び第2MACを第1ノードから受信することができ、その結果、第2ノードは、第2MACを使用することによって、暗号化された情報及び第2通信情報の完全性を検証する。これにより、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

10

【0031】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み；暗号化された情報は、暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、完全性保護アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することより取得され；方法は、完全性保護アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得するステップと；第4MACが前記第2MACと同じである場合、暗号化アルゴリズムを使用することによって、暗号化された情報を復号するステップと；を更に含む。前述の方法に基づいて、第2ノードは更に、完全性保護アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得し、第4MACを使用することによって、暗号化された情報及び第2通信情報の完全性を検証し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

20

【0032】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み；暗号化された情報は、認証された暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することにより取得され；方法は、認証された暗号化アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得するステップと；第4MACが第2MACと同じである場合、認証された暗号化アルゴリズムを使用することによって、暗号化された情報を復号するステップと；を更に含む。前述の方法に基づいて、第2ノードは更に、認証された暗号化アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得し、第4MACを使用することによって、暗号化された情報及び第2通信情報の完全性を検証し得る。これにより、第1ノードと第2ノードとの間の通信のセキュリティが向上する。

30

【0033】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、第1ノードによってサポートされ、かつ1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、少なくとも1つの第1KDFは、第1ノードによってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFである。前述の方法に基づいて、アルゴリズムの優先度はアルゴリズムのセキュリティに基づいて取得され、使用されるアルゴリズムの優先度が高いほど通信セキュリティが高いことを示すため、第2ノードは、第1ノードによってサポートされ、かつ1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムと、第1ノードによってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFを使用することによって、第1ノードと通信する。これにより、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

40

【0034】

50

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは1つ以上のアルゴリズムタイプに対応し、少なくとも1つの第1アルゴリズムに対応するアルゴリズムタイプは、第1ノードによってサポートされ、かつ1つ以上のアルゴリズムの1つ以上のアルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムタイプである。前述の方法に基づいて、第1ノードは、該第1ノードと第2ノードの両方によってサポートされるアルゴリズムタイプにおいて、最も高い優先度を有するアルゴリズムタイプを決定することができ、その結果、第1ノードは、最も高い優先度を有するアルゴリズムタイプに対応する少なくとも1つの第1アルゴリズムを決定する。

【0035】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは1つのアルゴリズムタイプに対応し、該アルゴリズムタイプは異なる優先度を有する複数のアルゴリズムに対応してよく、第1アルゴリズムは、第1ノードによってサポートされ、かつ上記のアルゴリズムタイプに対応するアルゴリズムにおいて最も高い優先度を有するアルゴリズムである。前述の方法に基づいて、少なくとも1つの第1アルゴリズムが1つのアルゴリズムタイプに対応するとき、第1ノードは、該第1ノードによってサポートされ、かつ第1アルゴリズムに対応するアルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムを、第1アルゴリズムとして決定し得る。あるいは、アルゴリズムタイプが1つのアルゴリズムのみに対応する場合、第1ノードは、第1アルゴリズムが、そのアルゴリズムを含むことを決定する。このようにして、第1ノードは、比較的高い優先度を有するアルゴリズムを使用することによって、第2ノードと通信し得る。通常、アルゴリズムの優先度は、アルゴリズムのセキュリティに関連する。したがって、第1ノードと第2ノードは、比較的高い優先度を有するアルゴリズムを使用することによって互いに通信し、その結果、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

【0036】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、少なくとも1つの第1アルゴリズムは、複数のアルゴリズムタイプに対応し、該複数のアルゴリズムタイプの優先度は同じである。各アルゴリズムタイプは、異なる優先度を有する1つ以上のアルゴリズムに対応してよく、少なくとも1つの第1アルゴリズムは、第1ノードによってサポートされ、かつ複数のアルゴリズムタイプの各々に対応するアルゴリズムにおいて最も高い優先度を有するアルゴリズムを含む。あるいは、アルゴリズムタイプが1つのアルゴリズムのみに対応する場合、少なくとも1つの第1アルゴリズムは、そのアルゴリズムタイプに対応するアルゴリズムを含む。前述の方法に基づいて、少なくとも1つの第1アルゴリズムが複数のアルゴリズムタイプに対応するとき、第1ノードは、第1ノードによってサポートされ、かつ各アルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムを第1アルゴリズムとして決定し得る。このようにして、第1ノードは、比較的高い優先度を有するアルゴリズムを使用することによって、第2ノードと通信し得る。通常、アルゴリズムの優先度は、アルゴリズムのセキュリティに関連する。したがって、第1ノードと第2ノードは、比較的高い優先度を有するアルゴリズムを使用することによって互いに通信し、その結果、第1ノードと第2ノードとの間の通信のセキュリティを向上させることができる。

【0037】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを更に含み、第2フレッシュパラメータは、第1アルゴリズムネゴシエーション要求情報の時間妥当性に関連するパラメータであり、方法は、第2検証情報を第1ノードに送信するステップを更に含み、第2検証情報は、第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて取得される。前述の方法に基づいて、第2ノードは、第2検証情報を使用することによって、第1情報に対して完全性保護を実行し得る。

【0038】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、方法は、第2アルゴリズムネゴシエーション要求情報を第1ノードに送信するステップであって、第2アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される、ステップと；第3情報を第1ノードから受信するステップであって、第3情報は、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFがサポートされていないか又は適用可能でないことを示すために使用される、ステップと；を更に含む。前述の方法に基づいて、第2ノードは、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される第2アルゴリズムネゴシエーション要求情報を第1ノードに送信し、第1ノードから、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFがサポートされていないか又は適用可能でないことを示すために使用される第3情報を受信し得る。このようにして、第1ノードと第2ノードは、通信を複数回行うことによってアルゴリズム及びKDFをネゴシエーションすることができ、第1ノードと第2ノードによるアルゴリズム及びKDFのネゴシエーションの成功率を改善することができる。

10

【0039】

第2の態様及び該第2の態様の可能な実装に関連して、ある可能な実装では、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムとは異なり；第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFとは異なる。前述の方法に基づいて、第2ノードは、1つ以上のアルゴリズム及び1つ以上のKDFを第1ノードに複数回示すことができ、その結果、第1ノードは、1つ以上の受信したアルゴリズム及び1つ以上の受信したKDFに基づいて、第2ノードとの通信に使用されるアルゴリズム及びKDFを決定する。これにより、第1ノードと第2ノードによるアルゴリズム及びKDFのネゴシエーションの成功率を改善する。

20

【0040】

第3の態様によると、本出願の実施形態は、第1の態様又は該第1の態様の可能な実装のうちのいずれか1つにおける方法を実装するために通信装置を提供する。当該装置は、方法を実行するよう構成される対応するユニット又は構成要素を含む。当該装置に含まれるユニットは、ソフトウェア及び／又はハードウェアによって実装され得る。例えば装置は、第1ノード又は前述の方法を実装する際に第1ノードをサポートすることができるチップ、チップシステム、プロセッサ等であり得る。

30

【0041】

第4の態様によると、本出願の実施形態は、第2の態様又は該第2の態様の可能な実装のうちのいずれか1つにおける方法を実装するために通信装置を提供する。当該装置は、方法を実行するよう構成される対応するユニット又は構成要素を含む。当該装置に含まれるユニットは、ソフトウェア及び／又はハードウェアによって実装され得る。例えば装置は、第2ノード又は前述の方法を実装する際に第2ノードをサポートすることができるチップ、チップシステム、プロセッサ等であり得る。

40

【0042】

第5の態様によると、本出願の実施形態は、プロセッサを含む通信装置を提供し、プロセッサはメモリに結合され、メモリは、プログラム又は命令を記憶するよう構成され、プログラム又は命令がプロセッサによって実行されると、当該装置は、第1の態様又は該第1の態様の可能な実装のうちのいずれか1つを実装することができる。

【0043】

第6の態様によると、本出願の実施形態は、プロセッサを含む通信装置を提供し、プロセッサはメモリに結合され、メモリは、プログラム又は命令を記憶するよう構成され、プログラム又は命令がプロセッサによって実行されると、当該装置は、第2の態様又は該第

50

2の態様の可能な実装のうちのいずれか1つを実装することができる。

【0044】

第7の態様によると、本出願の実施形態は、通信装置を提供する。当該装置は、第1の態様又は該第1の態様の可能な実装のうちのいずれか1つを実装するよう構成される。

【0045】

第8の態様によると、本出願の実施形態は、通信装置を提供する。当該装置は、第2の態様又は該第2の態様の可能な実装のうちのいずれか1つを実装するよう構成される。

【0046】

第9の態様によると、本出願の実施形態は、コンピュータ読取可能媒体を提供する。コンピュータ読取可能媒体は、コンピュータプログラム又は命令を記憶し、コンピュータプログラム又は命令が実行されると、コンピュータは、第1の態様又は該第1の態様の可能な実装のうちのいずれか1つにおける方法を実行することができる。

【0047】

第10の態様によると、本出願の実施形態は、コンピュータ読取可能媒体を提供する。コンピュータ読取可能媒体は、コンピュータプログラム又は命令を記憶し、コンピュータプログラム又は命令が実行されると、コンピュータは、第2の態様又は該第2の態様の可能な実装のうちのいずれか1つにおける方法を実行することができる。

【0048】

第11の態様によると、本出願の実施形態は、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は、コンピュータプログラムコードを含む。コンピュータプログラムコードがコンピュータ上で実行されると、該コンピュータは、第1の態様又は該第1の態様の可能な実装のうちのいずれか1つにおける方法を実行することができる。

【0049】

第12の態様によると、本出願の実施形態は、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は、コンピュータプログラムコードを含む。コンピュータプログラムコードがコンピュータ上で実行されると、該コンピュータは、第2の態様又は該第2の態様の可能な実装のうちのいずれか1つにおける方法を実行することができる。

【0050】

第13の態様によると、本出願の実施形態は、少なくとも1つのプロセッサを含むチップを提供し、プロセッサはメモリに結合され、メモリはプログラム又は命令を記憶するよう構成され、プログラム又は命令がプロセッサによって実行されると、チップは、第1の態様又は該第1の態様の可能な実装のうちのいずれか1つにおける方法を実装することができる。

【0051】

第14の態様によると、本出願の実施形態は、少なくとも1つのプロセッサを含むチップを提供し、プロセッサはメモリに結合され、メモリはプログラム又は命令を記憶するよう構成され、プログラム又は命令がプロセッサによって実行されると、チップは、第2の態様又は該第2の態様の可能な実装のうちのいずれか1つにおける方法を実装することができる。

【0052】

第15の態様によると、本出願の実施形態は、通信システムを提供する。当該システムは、第3の態様による装置及び／又は第4の態様による装置を含むか、当該システムは、第5の態様による装置及び／又は第6の態様による装置を含むか、当該システムは、第7の態様による装置及び／又は第8の態様による装置を含む。

【0053】

上記で提供される通信装置、チップ、コンピュータ読取可能媒体、コンピュータプログラム製品、通信システム等のいずれか1つが、上記で提供される、対応する方法を実行するよう構成されることが理解されよう。したがって、通信装置、チップ、コンピュータ読取可能媒体、コンピュータプログラム製品、通信システム等によって達成され得る有益な効果については、対応する方法における有益な効果を参照されたい。詳細は本明細書では

10

20

30

40

50

、説明されない。

【図面の簡単な説明】

【0054】

【図1】本出願の一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。

【0055】

【図2】本出願の一実施形態による通信装置のハードウェア構造の概略図である。

【0056】

【図3】本出願の一実施形態による通信方法の概略フローチャート1である。

【0057】

【図4】本出願の一実施形態による通信方法の概略フローチャート2である。

10

【0058】

【図5】本出願の一実施形態による通信方法の概略フローチャート3である。

【0059】

【図6】本出願の一実施形態による通信方法の概略フローチャート4である。

【0060】

【図7】本出願の一実施形態による通信方法の概略フローチャート5である。

【0061】

【図8】本出願の一実施形態による通信方法の概略フローチャート6である。

【0062】

【図9】本出願の一実施形態による通信装置の概略構造図1である。

20

【0063】

【図10】本出願の一実施形態による通信装置の概略構造図2である。

【0064】

【図11】本出願の一実施形態による通信装置の概略構造図3である。

【0065】

【図12】本出願の一実施形態による通信システムの概略構成図である。

【0066】

【図13】本出願の一実施形態によるチップの概略構造図である。

【発明を実施するための形態】

【0067】

30

以下は、添付の図面を参照して、本出願の実施形態の実装を詳細に説明する。

【0068】

本出願の実施形態において提供される方法は、様々な通信システムに適用され得る。例えば通信システムは、長期進化 (long term evolution、LTE) システム、第5世代 (5th generation、5G) 通信システム、新しい無線 (new radio、NR) システム、ワイヤレスフィデリティ (wireless fidelity、Wi-Fi) システム、第3世代パートナーシッププロジェクト (3rd generation partnership project、3GPP (登録商標)) に関連する通信システム及び将来展開される通信システムであり得る。これは限定されない。図1に示される通信システム10は単に、本出願の実施形態において提供される方法を説明するために一例として以下で使用される。

40

【0069】

図1は、本出願の一実施形態による通信システム10の概略アーキテクチャ図である。図1において、通信システム10は、ノード101と、該ノード101と通信することができるノード102を含み得る。図1は、概略図にすぎず、本出願で提供される技術的解決策の適用可能なシナリオに対する限定を構成するものではない。

【0070】

図1のノード101又はノード102は、受信及び送信機能を有する任意のデバイスであり得る。このデバイスは、LTEにおけるevolved NodeB (NodeB、eNB又はe-NodeB、evolutional Node B)、NRにおけるgN

50

odeB (gNodeB又はgNB)又は送信受信点 (transmission receiving point/transmission reception point、TRP)、3GPPからその後進化した基地局、Wi-Fiシステムにおけるアクセスノード、無線中継ノード、無線バックホールノード、データ転送デバイス (例えばルータ、中継器、ブリッジ又はスイッチ)等を含むが、これらに限定されない。基地局は、マクロ基地局、マイクロ基地局、ピコセル基地局、スモールセル、中継基地局、バルーン基地局等であり得る。あるいは、ノード101又はノード102は、クラウド無線アクセスネットワーク (cloud radio access network、CRAN) シナリオにおける無線コントローラ、集中ユニット (centralized unit、CU) 及び/又は分散ユニット (distributed unit、DU) であってもよい。あるいは、ノード101又はノード102は、サーバ、ウェアラブルデバイス (スマートウォッチ、スマートバンド又は歩数計等)、機械通信デバイス、車載デバイス等であってもよい。ノード101又はノード102は、携帯電話 (mobile phone)、タブレットコンピュータ (Pad)、無線送受信機能を有するコンピュータ、ヘッドセット、スピーカ、仮想現実 (virtual reality、VR) 端末デバイス、拡張現実 (augmented reality、AR)、機械型通信 (machine type communication、MTC) における端末、産業用制御 (industrial control) における端末、車載端末デバイス、自走式 (self driving) の端末、補助運転の端末デバイス、遠隔医療 (remote medical) における端末、スマートグリッド (smart grid) における端末、輸送安全性 (transportation safety) における端末、スマートシティ (smart city) の端末、スマートホーム (smart home) の端末等であり得る。適用シナリオは、本出願の実施形態において限定されない。端末は、端末デバイス、ユーザ機器 (user equipment、UE)、アクセス端末デバイス、車載端末、産業制御端末、UEユニット、UE局、移動局、移動コンソール、リモート局、リモート端末デバイス、モバイルデバイス、UE端末デバイス、無線通信デバイス、機械端末、UEエージェント、UE装置等とも呼ばれることがある。端末は固定式であっても移動式であってもよい。あるいは、ノード101又はノード102は、車両コックピットドメイン (cockpit domain) デバイス又は車両コックピットドメイン内のモジュール (コックピットドメインコントローラ (cockpit domain controller、CDC))、カメラ、スクリーン、マイクロホン、スピーカ、電子キー又は受動エントリ受動開始システムコントローラのような) であってもよい。

【0071】

図1に示される通信システム10は、単に一例として使用されるものであるが、本出願の技術的解決策を限定するよう意図されていない。当業者は、特定の実装プロセスにおいて、通信システム10が別のデバイスを更に含んでもよく、ノードの数量が特定の要件に基づいて決定されてよいことを理解すべきである。これに限定されない。

【0072】

任意に、本出願の実施形態では、ノード101又はノード102のような図1の各ノードは、装置内の機能モジュールであってもよい。機能モジュールは、ハードウェアデバイス内の要素、例えば端末デバイス又はネットワークデバイス内の通信チップ又は通信構成要素であってもよく、あるいはハードウェア上で動作するソフトウェア機能モジュール又はプラットフォーム (例えばクラウドプラットフォーム) 上でインスタンス化された仮想化機能であってもよいことが理解され得る。

【0073】

例えば図1の各ノードは、図2の通信装置200を使用することによって実装され得る。図2は、本出願の実施形態に適用可能な通信装置のハードウェア構造の概略図である。通信装置200は、少なくとも1つのプロセッサ201、メモリ203及び少なくとも1つの通信インタフェース204を含み得る。任意に、通信装置は、通信線202を更に含む。

10

20

30

40

50

【0074】

少なくとも1つのプロセッサ201は、汎用中央処理ユニット（central processing unit、CPU）、マイクロプロセッサ、特定用途向け集積回路（application-specific integrated circuit、ASIC）、フィールドプログラマブルゲートアレイ（Field Programmable Gate Array、FPGA）又は本出願の解決策においてプログラム実行を制御するよう構成される1つ以上の集積回路のうちの1つ以上を含み得る。

【0075】

通信線202は、前述の構成要素間で情報を送信するよう構成され得る。例えば通信線202はバスである。

【0076】

通信インタフェース204は、別のデバイス又は通信ネットワークと通信するよう構成され、イーサネット（登録商標）インタフェース、無線アクセスネットワーク（radio access network、RAN）インタフェース又は無線ローカルエリアネットワーク（wireless local area networks、WLAN）インタフェース等のようなトランシーバタイプの任意の装置である。あるいは、通信インタフェース204は、データ、命令又は情報の送信又は受信を完了するために、少なくとも1つのプロセッサ201に入力及び出力を提供し得る。しかしながら、接続構造は、図2に示されるものに限定されない。

【0077】

メモリ203は、静的情報及び命令を記憶することができる読取専用メモリ（read-only memory、ROM）又は別のタイプの静的ストレージデバイス、あるいは情報及び命令を記憶することができるランダムアクセスメモリ（random access memory、RAM）又は別のタイプの動的ストレージデバイスであってよく、あるいは電氣的消去可能なプログラマブル読取専用メモリ（electrically erasable programmable read-only memory、EEPROM）、コンパクトディスク読取専用メモリ（compact disc read-only memory、CD-ROM）又は他のコンパクトディスクストレージ、光ディスクストレージ（圧縮光ディスク、レーザディスク、光ディスク、デジタル多用途光ディスク、ブルーレイ（登録商標）ディスク等を含む）、磁気ディスク記憶媒体又は別の磁気記憶デバイス、あるいは予期されるプログラムコードを命令又はデータ構造の形態で担持又は記憶することができ、かつコンピュータによってアクセスされることができる任意の他の媒体であってよいが、これに限定されない。メモリは独立に存在してもよく、通信線202を介してプロセッサに接続される。あるいは、メモリは、プロセッサと一体化されてもよい。本出願の実施形態において提供されるメモリは、通常、不揮発性であり得る。メモリ203は、本出願の解決策を実行するためのコンピュータ実行可能命令を記憶するよう構成され、プロセッサ201は実行を制御する。プロセッサ201は、メモリ203に記憶されたコンピュータ実行可能命令を実行するよう構成され、本出願の実施形態に提供される方法を実装する。

【0078】

任意に、本出願の実施形態におけるコンピュータ実行可能命令は、アプリケーションプログラムコードとも呼ばれることがある。これは、本出願の実施態様において特に限定されない。

【0079】

特定の実装の間に、一実施形態では、プロセッサ201は、1つ以上のCPU、例えば図2のCPU0及びCPU1を含み得る。

【0080】

特定の実装の間に、一実施形態では、通信装置200は、複数のプロセッサ、例えば図2のプロセッサ201及びプロセッサ207を含み得る。プロセッサの各々は、シングルコア（シングルCPU）プロセッサであり得るか、マルチコア（マルチCPU）プロセッ

10

20

30

40

50

サであり得る。本明細書におけるプロセッサは、データ（例えばコンピュータプログラム命令）を処理するよう構成される1つ以上のデバイス、回路及び／又は処理コアを参照し得る。

【0081】

特定の実装の間に、一実施形態では、通信装置200は、出力デバイス205と入力デバイス206を更に含み得る。出力デバイス205は、プロセッサ201と通信し、複数の方式で情報を表示し得る。例えば出力デバイス205は、液晶ディスプレイ（liquid crystal display、LCD）、発光ダイオード（light-emitting diode、LED）ディスプレイデバイス、陰極線管（cathode ray tube、CRT）ディスプレイデバイス又はプロジェクタ（projector）であり得る。入力デバイス206は、プロセッサ201と通信し、複数の方式でユーザから入力を受信し得る。例えば入力デバイス206は、マウス、キーボード、タッチスクリーンデバイス又は感知デバイスであり得る。

10

【0082】

特定の実装の間に、通信装置200は、デスクトップコンピュータ、ポータブルコンピュータ、ネットワークサーバ、パーソナルデジタルアシスタント（personal digital assistant、PDA）、携帯電話、タブレットコンピュータ、無線端末デバイス、内蔵デバイス又は図2と同様の構造を有するデバイスであり得る。通信装置200のタイプは、本出願の実施形態では限定されない。

【0083】

以下では、図1及び図2を参照して、本出願の実施形態における通信方法を具体的に説明する。以下の実施形態におけるノードは、図2に示される構成要素を有し得る。

20

【0084】

本出願の実施形態におけるアルゴリズムは、シグナリングプレーン（signaling plane）アルゴリズム、ユーザプレーン（user plane）アルゴリズム又はシグナリングプレーンアルゴリズムとユーザプレーンアルゴリズムであり得ることに留意されたい。シグナリングプレーンは、制御型シグナリング（control-type signaling）、例えばアクセス要求情報又はアイデンティティ認証情報を送信するために使用され、ユーザプレーンは、データを送信するために使用される。シグナリングプレーンアルゴリズムは、第1ノードと第2ノードとの間のシグナリングプレーン通信に使用される。シグナリングプレーンアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含み得る。ユーザプレーンアルゴリズムは、第1ノードと第2ノードとの間のユーザプレーン通信に使用される。ユーザプレーンアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含み得る。

30

【0085】

本出願の実施形態において、ユーザプレーンアルゴリズムは、シグナリングプレーンアルゴリズムと同じであってよく、あるいはシグナリングプレーンアルゴリズムとは異なってもよい。シグナリングプレーンアルゴリズムが、ユーザプレーンアルゴリズムと同じであることは、以下のように表され得る：シグナリングプレーンアルゴリズムの数量が、ユーザプレーンアルゴリズムの数量と同じであり、シグナリングプレーンアルゴリズムのタイプが、ユーザプレーンアルゴリズムのタイプと同じであり、シグナリングプレーンアルゴリズムの識別子が、ユーザプレーンアルゴリズムの識別子と同じである。例えば2つのシグナリングプレーンアルゴリズム：暗号化アルゴリズム1と完全性保護アルゴリズム1が存在し、また2つのユーザプレーンアルゴリズム：暗号化アルゴリズム1と完全性保護アルゴリズム1も存在する。シグナリングプレーンアルゴリズムが、ユーザプレーンアルゴリズムと異なることは、以下のように表され得る：シグナリングプレーンアルゴリズムのタイプが、ユーザプレーンアルゴリズムのタイプと異なり（例えばシグナリングプレーンアルゴリズムが、暗号化アルゴリズムと完全性保護アルゴリズムを含み、ユーザプレーンアルゴリズムが、認証された暗号化アルゴリズムを含む）、及び／又はシグナリン

40

50

グプレーンアルゴリズムの数量が、ユーザプレーンアルゴリズムの数量と異なる（例えば2つのシグナリングプレーンアルゴリズムが存在し、1つのユーザプレーンアルゴリズムが存在する）か；あるいはシグナリングプレーンアルゴリズムのタイプがユーザプレーンアルゴリズムのタイプと同じであり、シグナリングプレーンアルゴリズムの数量がユーザプレーンアルゴリズムの数量と同じであるとき、シグナリングプレーンアルゴリズムの識別子が、ユーザプレーンアルゴリズムの識別子と異なる（例えば2つのシグナリングプレーンアルゴリズム：暗号化アルゴリズム1と完全性保護アルゴリズム1が存在し、2つのユーザプレーンアルゴリズム：暗号化アルゴリズム2と完全性保護アルゴリズム2が存在する）。

【0086】

本出願の以下の実施態様において、ノード間のメッセージの名前、メッセージ内の各パラメータの名前等は、単なる例示であり、特定の実装の間では代替的に別の名前であってもよいことに留意されたい。これは、本出願の実施態様において特に限定されない。

【0087】

本出願の実施形態において、第1ノード又は第2ノードは、本出願の実施形態におけるステップの一部又はすべてを実行し得ることが理解され得る。これらのステップは単なる例である。本出願の実施形態において、他のステップ又は様々なステップの変形が代替的に実行されてもよい。加えて、ステップは、本出願の実施形態において提示される順序とは異なる順序で実行されてよく、本出願の実施形態におけるステップの必ずしもすべてが実行される必要がない可能性がある。

【0088】

図3は、本出願の一実施形態による通信方法を示す。通信方法は、ステップ301～ステップ303を含む。

【0089】

ステップ301：第2ノードが、第1アルゴリズムネゴシエーション要求情報を第1ノードに送信する。

【0090】

第2ノードは、図1の任意のノードであってよい。例えば第2ノードは、図1に示されるノード101又はノード102であり得る。第2ノードが、図1に示されるノード101であるとき、第1ノードは、図1に示されるノード102であり得る。第2ノードが、図1に示されるノード102であるとき、第1ノードは、図1に示されるノード101であり得る。

【0091】

第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上の鍵導出関数（`key derivation function`、`KDF`）を示すために使用され得る。1つ以上のアルゴリズムは、第2ノードによってサポートされる1つ以上のアルゴリズムであり得る。1つ以上の`KDF`は、第2ノードによってサポートされる1つ以上の`KDF`であり得る。`KDF`は、1つ以上のアルゴリズムの一部又はすべてに対応する鍵を生成するために使用され得る。

【0092】

本明細書では、第2ノードによってサポートされる1つ以上のアルゴリズム及び／又は第2ノードによってサポートされる1つ以上の`KDF`は、第2ノードのセキュリティ能力と総称されることがあることに留意されたい。

【0093】

1つ以上のアルゴリズムは、同じタイプのアルゴリズムであってよく、あるいは異なるタイプのアルゴリズムであってもよい。例えば1つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む。さらに、1つ以上のアルゴリズムは、少なくとも1つの暗号化アルゴリズム及び／又は少なくとも1つの完全性保護アルゴリズム及び／又は少なくとも1つの認証された暗号化アルゴリズムを含む。暗号化アルゴリズムは、該暗号化アルゴリズムの鍵を使用するこ

10

20

30

40

50

とによって第1ノードと第2ノードとの間の通信情報の一部又はすべてを暗号化又は復号するために使用され得る。完全性保護アルゴリズムは、該完全性保護アルゴリズムに対応する鍵を使用することによって、第1ノードと第2ノードとの間の通信情報の一部又はすべてに対して完全性保護を実行するため、あるいは完全性保護アルゴリズムに対応する鍵を使用することによって、第1ノードと第2ノードとの間の通信情報の一部又はすべての完全性を検証するために、使用され得る。認証された暗号化アルゴリズムは、該認証された暗号化アルゴリズムの鍵を使用することによって、第1ノードと第2ノードとの間の通信情報の一部又はすべてを暗号化又は復号するために使用されてよく、認証された暗号化アルゴリズムは、該認証された暗号化アルゴリズムの鍵を使用することによって、第1ノードと第2ノードとの間の通信情報の一部又はすべてに対して完全性保護を実行するため、あるいは認証された暗号化アルゴリズムの鍵を使用することによって、第1ノードと第2ノードとの間の通信情報の一部又はすべての完全性を検証するために、使用され得る。

10

【0094】

第1アルゴリズムネゴシエーション要求情報によって示される暗号化アルゴリズム、完全性保護アルゴリズム又は認証された暗号化アルゴリズムの数量は、本出願のこの実施形態において限定されないことが理解され得る。例えば第1アルゴリズムネゴシエーション要求情報は、8つのアルゴリズムを示すことができ、8つのアルゴリズムは、2つの暗号化アルゴリズムと、3つの完全性保護アルゴリズムと、3つの認証された暗号化アルゴリズムを含む。

【0095】

20

任意に、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度に基づいてソートされる。例えば第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度の降順にソートされるか、あるいは第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度の昇順にソートされる。

【0096】

例えば第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度の降順にソートされる。第1アルゴリズムネゴシエーション要求情報が、暗号化アルゴリズム1、暗号化アルゴリズム2、完全性保護アルゴリズム1、完全性保護アルゴリズム2、KDF1及びKDF2を示すために使用される場合、暗号化アルゴリズムの優先度は、完全性保護アルゴリズムの優先度以上である。暗号化アルゴリズムでは、暗号化アルゴリズム1の優先度は、暗号化アルゴリズム2の優先度以上である。完全性保護アルゴリズムでは、完全性保護アルゴリズム1の優先度は、完全性保護アルゴリズム2の優先度以上である。KDFでは、KDF1の優先度は、KDF2の優先度以上である。

30

【0097】

例えば第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度の昇順にソートされる。第1アルゴリズムネゴシエーション要求情報が、暗号化アルゴリズム1、暗号化アルゴリズム2、完全性保護アルゴリズム1、完全性保護アルゴリズム2、KDF1及びKDF2を示すために使用される場合、暗号化アルゴリズムの優先度は、完全性保護アルゴリズムの優先度以下である。暗号化アルゴリズムでは、暗号化アルゴリズム1の優先度は、暗号化アルゴリズム2の優先度以下である。完全性保護アルゴリズムでは、完全性保護アルゴリズム1の優先度は、完全性保護アルゴリズム2の優先度以下である。KDFでは、KDF1の優先度は、KDF2の優先度以下である。

40

【0098】

1つ以上のアルゴリズムがシグナリングプレーンアルゴリズムとユーザプレーンアルゴリズムの両方を含む場合、1つ以上のアルゴリズムは、シグナリングプレーンアルゴリズムの優先度とユーザプレーンアルゴリズムの優先度に基づいて別々にソートされることが

50

理解され得る。

【0099】

例えば第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度の降順にソートされる。第1アルゴリズムネゴシエーション要求情報によって示されるアルゴリズム及びKDFは表1に示され得ることが想定される。表1では、ユーザプレーンアルゴリズムは、暗号化アルゴリズム1、暗号化アルゴリズム2及び完全性保護アルゴリズム1を含み、シグナリングプレーンアルゴリズムは、暗号化アルゴリズム2、完全性保護アルゴリズム1及び完全性保護アルゴリズム2を含み、KDFは、KDF1、KDF2及びKDF3を含む。このケースでは、ユーザプレーンアルゴリズム及びシグナリングプレーンアルゴリズムでは、暗号化アルゴリズムの優先度は、完全性保護アルゴリズムの優先度以上である。ユーザプレーンアルゴリズムに含まれる暗号化アルゴリズムでは、暗号化アルゴリズム1の優先度は、暗号化アルゴリズム2の優先度以上である。シグナリングプレーンアルゴリズムに含まれる完全性保護アルゴリズムでは、完全性保護アルゴリズム1の優先度は、完全性保護アルゴリズム2の優先度以上である。

10

【表1】

表1

ユーザプレーンアルゴリズム	シグナリングプレーンアルゴリズム	KDF
暗号化アルゴリズム1	アルゴリズム2	KDF1
暗号化アルゴリズム2	完全性保護アルゴリズム1	KDF2
完全性保護アルゴリズム1	完全性保護アルゴリズム2	KDF3

20

【0100】

例えば第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFは、優先度の降順にソートされる。第1アルゴリズムネゴシエーション要求情報によって示されるアルゴリズム及びKDFは、代替的に表2に示され得る。表2では、ユーザプレーンアルゴリズム／KDFについて、認証された暗号化アルゴリズムの優先度は、暗号化アルゴリズム及び完全性保護アルゴリズムの優先度より高く、暗号化アルゴリズムと完全性保護アルゴリズムの優先度は同じである。ここで、認証された暗号化アルゴリズム1の優先度は、認証された暗号化アルゴリズム2の優先度以上であり、完全性保護アルゴリズム1の優先度は、完全性保護アルゴリズム2の優先度以上であり、完全性保護アルゴリズム2の優先度は、暗号化アルゴリズム1の優先度以上であり、暗号化アルゴリズム1の優先度は、暗号化アルゴリズム2の優先度以上であり、KDF1の優先度は、KDF2の優先度以上である。シグナリングプレーンアルゴリズム／KDFについて、暗号化アルゴリズムと完全性保護アルゴリズムの優先度は同じであり、暗号化アルゴリズムと完全性保護アルゴリズムの優先度は、認証された暗号化アルゴリズムの優先度よりも高い。ここで、完全性保護アルゴリズム1の優先度は、完全性保護アルゴリズム2の優先度以上であり、完全性保護アルゴリズム2の優先度は、暗号化アルゴリズム1の優先度以上であり、暗号化アルゴリズム1の優先度は、暗号化アルゴリズム2の優先度以上であり、認証された暗号化アルゴリズム2の優先度は、認証された暗号化アルゴリズム1の優先度以上であり、KDF3の優先度は、KDF4の優先度以上である。

30

40

50

【表 2】

表 2

ユーザプレーン アルゴリズム ／KDF 優先度	ユーザプレーン アルゴリズム／KDF 識別子	シグナリングプ レーンアルゴリ ズム／KDF 優先度	シグナリングプレーン アルゴリズム／KDF 識別子
優先度 1	認証された暗号化アルゴリズム 1	優先度 1	完全性保護アルゴリズム 1
	認証された暗号化アルゴリズム 2		完全性保護アルゴリズム 2
優先度 2	完全性保護アルゴリズム 1		暗号化アルゴリズム 1
	完全性保護アルゴリズム 2		暗号化アルゴリズム 2
	暗号化アルゴリズム 1	優先度 2	認証された暗号化アルゴリズム 2
	暗号化アルゴリズム 2		認証された暗号化アルゴリズム 1
KDF 優先度	KDF 1	KDF 優先度	KDF 3
	KDF 2		KDF 4

10

20

【0101】

第 1 アルゴリズムネゴシエーション要求情報は、1 つ以上のアルゴリズム及び 1 つ以上の KDF を以下の方式のうちのいずれか 1 つで示すことができる。

【0102】

方式 1.1：第 1 アルゴリズムネゴシエーション要求情報は、1 つ以上のアルゴリズムの 1 つ以上の識別子と、1 つ以上の KDF の 1 つ以上の識別子を含む。

【0103】

例えば表 3 に示されるアルゴリズム／KDF 識別子を例として用いる。第 1 アルゴリズムネゴシエーション要求情報が ID 1、ID 3 及び ID 5 を含むとき、第 1 アルゴリズムネゴシエーション要求情報は、アルゴリズム 1、アルゴリズム 3 及び KDF 2 を示すために使用される。第 1 アルゴリズムネゴシエーション要求情報が ID 2 と ID 4 を含むとき、第 1 アルゴリズムネゴシエーション要求情報は、アルゴリズム 2 と KDF 1 を示すために使用される。

30

【表 3】

表 3

アルゴリズム／KDF	アルゴリズム／KDF 識別子
アルゴリズム 1	ID 1
アルゴリズム 2	ID 2
アルゴリズム 3	ID 3
KDF 1	ID 4
KDF 2	ID 5

40

【0104】

表 1～表 3 は、第 1 アルゴリズムネゴシエーション要求情報によって示されるアルゴリ

50

ズムの単なる例であることが理解され得る。特定の適用において、第1アルゴリズムネゴシエーション要求情報によって示されるアルゴリズムは、代替的に、他の形式であってもよい。これは限定されない。

【0105】

方式1.2：第1アルゴリズムネゴシエーション要求情報は、1つのビットシーケンスを含み、該ビットシーケンス内の1つのビットは、1つのアルゴリズム又は1つのKDFに対応し、ビットシーケンス内の各ビットは、0又は1を使用することによって、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するアルゴリズムを示すか又はKDFを示すかを指示することができる。例えばビットが1である場合、これは、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するアルゴリズム又はKDFを示すことを指示することができ、ビットが0である場合、これは、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するアルゴリズム又はKDFを示さないことを指示することができ、逆も同様である。

10

【0106】

例えば第1アルゴリズムネゴシエーション要求情報は5ビットを含み、5ビット内において、第1ビットはアルゴリズム1に対応し、第2ビットはアルゴリズム2に対応し、第3ビットはアルゴリズム3に対応し、第4ビットはKDF1に対応し、第5ビットはKDF2に対応する。5ビットが01010である場合、これは、第1アルゴリズムネゴシエーション要求情報が、アルゴリズム2及びKDF1を示すために使用されることを指示し得る。5ビットが11001である場合、これは、第1アルゴリズムネゴシエーション要求情報が、アルゴリズム1、アルゴリズム2及びKDF2を示すため使用されることを指示し得る。

20

【0107】

方式1.3：第1アルゴリズムネゴシエーション要求情報は、2つのビットシーケンスを含み、ここで、2つのビットシーケンスの長さは、同じであっても、異なってもよい。

【0108】

ビットシーケンスのうちの一方のビットシーケンスについて、該ビットシーケンス内の1ビットは1つのアルゴリズムに対応し、ビットシーケンス内の各ビットは、0又は1を使用することによって、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するアルゴリズムを示すかどうかを指示し得る。例えばビットが1である場合、これは、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するアルゴリズムを示すことを指示することができ、ビットが0である場合、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するアルゴリズムを示さないことを指示することができ、逆も同様である。

30

【0109】

ビットシーケンスの他方のビットシーケンスについて、該ビットシーケンス内の1ビットは1つのKDFに対応し、ビットシーケンス内の各ビットは、0又は1を使用することによって、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するKDFを示すかどうかを指示し得る。例えばビットが1である場合、これは、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するKDFを示すことを指示することができ、ビットが0である場合、これは、第1アルゴリズムネゴシエーション要求情報が、そのビットに対応するKDFを示さないことを指示することができ、その逆も同様である。

40

【0110】

例えば第1アルゴリズムネゴシエーション要求情報は、2つのビットシーケンスを含み、該ビットシーケンスのうちの一方のビットシーケンスは3ビットを含み、3ビット内の第1ビットはアルゴリズム1に対応し、3ビット内の第2ビットはアルゴリズム2に対応し、3ビット内の第3ビットはアルゴリズム3に対応し、ビットシーケンスのうちの他方のビットシーケンスは2ビットを含み、2ビット内の第1ビットはKDF1に対応し、2ビット内の第2ビットはKDF2に対応する。第1アルゴリズムネゴシエーション要求情報が110及び01を含む場合、これは、第1アルゴリズムネゴシエーション要求情報が

50

アルゴリズム 1、アルゴリズム 2 及び K D F 2 を示すために使用されることを指示し得る。第 1 アルゴリズムネゴシエーション要求情報が 0 1 0 及び 1 1 を含む場合、これは、第 1 アルゴリズムネゴシエーション要求情報が、アルゴリズム 2、K D F 1 及び K D F 2 を示すために使用されることを指示し得る。

【0 1 1 1】

任意に、第 1 アルゴリズムネゴシエーション要求情報は、第 2 ノードの識別子と、第 2 フレッシュパラメータを更に含む。

【0 1 1 2】

第 2 ノードの識別子は、第 2 ノードを識別するために使用され得る。第 2 フレッシュパラメータは、第 1 アルゴリズムネゴシエーション要求情報の時間妥当性に関連するパラメータである。例えば第 2 フレッシュパラメータは、第 2 ノード内のカウンタの値又は第 1 ナンスを含む。カウンタの値は、第 2 ノードのカウンタのものであり、かつ第 2 ノードが第 1 アルゴリズムネゴシエーション要求情報を送信することを決定したときに存在する値とすることができ、カウンタは、第 1 ノードと第 2 ノードとの間の通信の時間の量を記録するために使用され得る。第 1 ナンスは、第 2 ノードが第 1 アルゴリズムネゴシエーション要求情報を送信することを決定したときに、第 2 ノードによって生成されるナンスであることができる。

【0 1 1 3】

任意に、ステップ 3 0 1 の前に、第 2 ノードは、該第 2 ノードが、第 1 ノードとネゴシエーションされるアルゴリズム及び K D F を有するかどうかを検出する。第 2 ノードが第 1 ノードとネゴシエーションされるアルゴリズム及び K D F を有する場合、第 2 ノードは、ネゴシエーションされるアルゴリズム及び K D F を使用することによって、第 1 ノードと通信する。第 2 ノードが、第 1 ノードとネゴシエーションされるアルゴリズム又は K D F を有しない場合、第 2 ノードはステップ 3 0 1 を実行する。

【0 1 1 4】

ステップ 3 0 2：第 1 ノードは、第 2 ノードから第 1 アルゴリズムネゴシエーション要求情報を受信し、1 つ以上のアルゴリズムにおける少なくとも 1 つの第 1 アルゴリズムと、1 つ以上の K D F における少なくとも 1 つの第 1 K D F を決定する。

【0 1 1 5】

本明細書では、第 1 ノードによってサポートされる 1 つ以上のアルゴリズム及び／又は第 1 ノードによってサポートされる 1 つ以上の K D F は、第 1 ノードのセキュリティ能力と総称されることがあることに留意されたい。

【0 1 1 6】

任意に、少なくとも 1 つの第 1 アルゴリズムは、暗号化アルゴリズムを含むか；少なくとも 1 つの第 1 アルゴリズムは、完全性保護アルゴリズムを含むか；少なくとも 1 つの第 1 アルゴリズムは、暗号化アルゴリズムと完全性保護アルゴリズムを含むか；あるいは、少なくとも 1 つの第 1 アルゴリズムは、認証された暗号化アルゴリズムを含む。

【0 1 1 7】

任意に、複数のアルゴリズムは、対応する優先度に対応する。複数の K D F は、対応する優先度に対応する。

【0 1 1 8】

可能な実装では、第 1 アルゴリズムネゴシエーション要求情報によって示される 1 つ以上のアルゴリズム及び 1 つ以上の K D F が、優先度に基づいてソートされる。詳細については、ステップ 3 0 1 の説明を参照されたい。詳細は再度説明しない。

【0 1 1 9】

別の可能な実装では、アルゴリズムの識別子とアルゴリズムの優先度との間に対応が存在する。任意に、その対応は、プリセットされ、例えば規格又はプロトコルで定義され、あるいは、その対応は、任意の他のデバイスを使用することによって、対応するノードについて、プリセットされて予め構成され得る。例えばより大きな識別子を有するアルゴリズムの優先度は、より小さな識別子を持つアルゴリズムの優先度よりも高い。あるいは、

10

20

30

40

50

より小さな識別子を有するアルゴリズムの優先度は、より大きな識別子を有するアルゴリズムの優先度よりも高い。例えばアルゴリズム 2 の優先度は、アルゴリズム 1 の優先度よりも高い。あるいは、アルゴリズム 1 の優先度は、アルゴリズム 2 の優先度よりも高い。同様に、K D F の識別子と K D F の優先度との間にも対応が存在する。例えばより大きい識別子を有する K D F の優先度は、より小さい識別子を有する K D F の優先度よりも高い。あるいは、より小さい識別子を有する K D F の優先度は、より大きい識別子を有する K D F の優先度よりも高い。説明を容易性のために、対応は、主にリスト方式で以下に説明される。しかしながら、当業者には、本出願は、表方式で通信を提示することを含むが、これに限定されないことがわかり得る。

【0120】

更に別の可能な実装では、複数のアルゴリズムの優先度が、アルゴリズム優先度リストを使用することによって提示される。複数の K D F の優先度は、K D F 優先度リストを使用することによって提示される。

【0121】

任意に、アルゴリズム優先度リストは、暗号化アルゴリズム優先度リスト及び／又は完全性保護アルゴリズム優先度リスト及び／又は認証された暗号化アルゴリズム優先度リストを含む。

【0122】

本出願のこの実施形態のアルゴリズムがシグナリングプレーンアルゴリズム及びユーザプレーンアルゴリズムである場合、アルゴリズム優先度リストは、ユーザプレーンアルゴリズム優先度リスト及び／又はシグナリングプレーンアルゴリズム優先度リストを含むことが理解され得る。ユーザプレーンアルゴリズム優先度リストは、ユーザプレーンの第 1 アルゴリズムを決定するために使用されてよく、シグナリングプレーンアルゴリズム優先度リストは、シグナリングプレーンの第 1 アルゴリズムを決定するために使用されてよい。ユーザプレーンアルゴリズム優先度リストとシグナリングプレーンアルゴリズム優先度リストは、同じであっても、異なってもよい。

【0123】

アルゴリズム優先度リストは、1 つ以上のアルゴリズムを含み、アルゴリズム優先度リストに含まれる 1 つ以上のアルゴリズムは、アルゴリズムの優先度に基づいてソートされることが理解され得る。例えば暗号化アルゴリズムの優先度リストを例として用いる。暗号化アルゴリズム優先度リストは、アルゴリズム 1、アルゴリズム 2 及びアルゴリズム 3 を含み、アルゴリズム 1 の優先度 $\geq$ アルゴリズム 2 の優先度 $\geq$ アルゴリズム 3 の優先度であるか又はアルゴリズム 1 の優先度 $\leq$ アルゴリズム 2 の優先度 $\leq$ アルゴリズム 3 の優先度である。K D F 優先度リストは、1 つ以上の K D F を含み、1 つ以上の K D F は、K D F の優先度に基づいてソートされる。例えば K D F 優先度リストは、K D F 1、K D F 2 及び K D F 3 を含み、K D F 1 の優先度 $\geq$ K D F 2 の優先度 $\geq$ K D F 3 の優先度であるか又は K D F 1 の優先度 $\leq$ K D F 2 の優先度 $\leq$ K D F 3 の優先度である。

【0124】

任意に、アルゴリズム優先度リスト内のアルゴリズムは、アルゴリズムの優先度の降順又は昇順でソートされる。K D F 優先度リスト内の K D F は、K D F の優先度の降順又は昇順にソートされる。

【0125】

例えばアルゴリズム優先度リストは、暗号化アルゴリズム優先度リスト、完全性保護アルゴリズム優先度リスト及び認証された暗号化アルゴリズム優先度リストを含み、認証された暗号化アルゴリズムの優先度 $>$ 完全性保護アルゴリズムの優先度 $\geq$ 暗号化アルゴリズムの優先度であり、暗号化アルゴリズム優先度リストは、アルゴリズム 1 及びアルゴリズム 2 を含み、アルゴリズム 1 の優先度はアルゴリズム 2 の優先度よりも高く、完全性保護アルゴリズム優先度リストはアルゴリズム 3 及びアルゴリズム 4 を含み、アルゴリズム 3 の優先度はアルゴリズム 4 の優先度よりも高く、認証された暗号化アルゴリズム優先度リストはアルゴリズム 5 及びアルゴリズム 6 を含み、アルゴリズム 5 の優先度はアルゴリズ

10

20

30

40

50

ム 6 の優先度よりも高く、各優先度リスト内のアルゴリズムはアルゴリズムの優先度の降順にソートされる。アルゴリズム優先度リストは、表 4 に示され得る。表 4 は、アルゴリズム優先度リストの単なる例であり、アルゴリズム優先度リストは、代替的に別の形態であってもよい。これは限定されない。

【表 4】

表 4

アルゴリズムタイプ	アルゴリズム識別子
認証された暗号化アルゴリズム	アルゴリズム 5
	アルゴリズム 6
完全性保護アルゴリズム	アルゴリズム 3
	アルゴリズム 4
暗号化アルゴリズム	アルゴリズム 1
	アルゴリズム 2

10

【0 1 2 6】

前述の例について、完全性保護アルゴリズムの優先度が暗号化アルゴリズムの優先度と同じであるとき、アルゴリズム優先度リストは表 5 に示され得ることが理解され得る。表 5 では、認証された暗号化アルゴリズムの優先度は優先度 1 であり、暗号化アルゴリズムの優先度と完全性保護アルゴリズムの優先度は優先度 2 であり、優先度 1 は優先度 2 より高い。

20

【表 5】

表 5

アルゴリズム優先度	アルゴリズムタイプ	アルゴリズム識別子
優先度 1	認証された暗号化アルゴリズム	アルゴリズム 5
		アルゴリズム 6
優先度 2	完全性保護アルゴリズム	アルゴリズム 3
		アルゴリズム 4
	暗号化アルゴリズム	アルゴリズム 1
		アルゴリズム 2

30

【0 1 2 7】

任意に、少なくとも 1 つの第 1 アルゴリズムは、第 1 ノードによってサポートされ、かつ 1 つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムである。少なくとも 1 つの第 1 アルゴリズムは、1 つ以上のアルゴリズムタイプに対応する。例えば少なくとも 1 つの第 1 アルゴリズムが 1 つのアルゴリズムを含む場合、少なくとも 1 つの第 1 アルゴリズムは、1 つのアルゴリズムタイプに対応する。少なくとも 1 つの第 1 アルゴリズムが複数のアルゴリズムを含む場合、少なくとも 1 つの第 1 アルゴリズムに含まれる複数のアルゴリズムの各々は、1 つのアルゴリズムタイプに対応する。

40

【0 1 2 8】

さらに、少なくとも 1 つの第 1 アルゴリズムに対応するアルゴリズムタイプは、第 1 ノードによってサポートされ、かつ 1 つ以上のアルゴリズムのアルゴリズムタイプにおいて最も高い優先度を有するアルゴリズムタイプである。

50

【0129】

可能な実装では、少なくとも1つの第1アルゴリズムは1つのアルゴリズムタイプに対応し、アルゴリズムタイプは異なる優先度を有する複数のアルゴリズムに対応してよく、第1アルゴリズムは、第1ノードによってサポートされ、かつそのアルゴリズムタイプに対応するアルゴリズムにおいて最も高い優先度を有するアルゴリズムである。あるいは、アルゴリズムタイプが1つのアルゴリズムのみに対応する場合、第1アルゴリズムは、そのアルゴリズムタイプに対応するアルゴリズムを含む。

【0130】

例えば少なくとも1つの第1アルゴリズムは1つのアルゴリズムを含み、第1アルゴリズムネゴシエーション要求情報は、アルゴリズム3、アルゴリズム4、アルゴリズム1及びアルゴリズム2を示し、アルゴリズム3の優先度>アルゴリズム4の優先度>アルゴリズム1の優先度>アルゴリズム2の優先度である。第1ノードによってサポートされるアルゴリズムがアルゴリズム4及びアルゴリズム1を含む場合、少なくとも1つの第1アルゴリズムはアルゴリズム4である。第1ノードによってサポートされるアルゴリズムがアルゴリズム3及びアルゴリズム1を含む場合、少なくとも1つの第1アルゴリズムはアルゴリズム3である。

【0131】

例えば少なくとも1つの第1アルゴリズムは1つのアルゴリズムを含み、アルゴリズム優先度リストは表5に示され、第1アルゴリズムネゴシエーション要求情報はアルゴリズム5、アルゴリズム6、アルゴリズム3及びアルゴリズム2を示す。第1ノードによってサポートされるアルゴリズムがアルゴリズム6、アルゴリズム3及びアルゴリズム1を含む場合、少なくとも1つの第1アルゴリズムはアルゴリズム6である。第1ノードによってサポートされるアルゴリズムがアルゴリズム5、アルゴリズム4及びアルゴリズム2を含む場合、少なくとも1つの第1アルゴリズムはアルゴリズム5である。

【0132】

別の可能な実装において、少なくとも1つの第1アルゴリズムは、複数のアルゴリズムタイプに対応し、該複数のアルゴリズムタイプの優先度は同じである。各アルゴリズムタイプは、異なる優先度を有する1つ以上のアルゴリズムに対応してよく、少なくとも1つの第1アルゴリズムは、第1ノードによってサポートされ、かつ複数のアルゴリズムタイプの各々に対応するアルゴリズムにおいて最も高い優先度を有するアルゴリズムを含む。あるいは、アルゴリズムタイプが1つのアルゴリズムのみに対応する場合、少なくとも1つの第1アルゴリズムは、そのアルゴリズムタイプに対応するアルゴリズムを含む。

【0133】

例えば少なくとも1つの第1アルゴリズムは、2つのアルゴリズムを含み、アルゴリズム優先度リストは、表6に示され、第1アルゴリズムネゴシエーション要求情報は、アルゴリズム5、アルゴリズム6、アルゴリズム3及びアルゴリズム2を示す。表6では、アルゴリズムタイプについて、暗号化アルゴリズムと完全性保護アルゴリズムの優先度は同じであり、暗号化アルゴリズムと完全性保護アルゴリズムの優先度は、認証された暗号化アルゴリズムの優先度よりも高い。暗号化アルゴリズムでは、アルゴリズム5の優先度は、アルゴリズム6の優先度以上である。完全性保護アルゴリズムでは、アルゴリズム3の優先度は、アルゴリズム4の優先度以上である。認証された暗号化アルゴリズムでは、アルゴリズム1の優先度は、アルゴリズム2の優先度以上である。第1ノードによってサポートされるアルゴリズムがアルゴリズム5、アルゴリズム6、アルゴリズム3、アルゴリズム4及びアルゴリズム1を含む場合、少なくとも1つの第1アルゴリズムは、アルゴリズム5及びアルゴリズム3を含む。

10

20

30

40

50

【表 6】

表6

優先度	アルゴリズムタイプ	アルゴリズム識別子
優先度 1	暗号化アルゴリズム	アルゴリズム 5
		アルゴリズム 6
	完全性保護アルゴリズム	アルゴリズム 3
		アルゴリズム 4
優先度 2	認証された暗号化アルゴリズム	アルゴリズム 1
		アルゴリズム 2

10

【0134】

第1アルゴリズムネゴシエーション要求情報によって示されるアルゴリズムのアルゴリズムタイプにおいて、最も高い優先度を有するアルゴリズムタイプが複数存在するとき、第1ノードは、複数のアルゴリズムタイプのうちの一部を、少なくとも1つの第1アルゴリズムに対応するアルゴリズムタイプとして決定し得ることに留意されたい。例えば第1アルゴリズムネゴシエーション要求情報によって示されるアルゴリズムのアルゴリズムタイプにおいて、最も高い優先度を有するアルゴリズムタイプは、暗号化アルゴリズムと完全性保護アルゴリズムであり、第1ノードは、完全性保護アルゴリズムを、少なくとも1つの第1アルゴリズムに対応するアルゴリズムタイプとして決定する。このシナリオでは、暗号化は、暗号化アルゴリズムを使用することによって実行されないことがある。解決策の説明の容易性のために、「アルゴリズムタイプを決定する」という表現が使用されることに更に留意されたい。しかしながら、実際の解決策では、アルゴリズムタイプは別々に決定されないことがあるが、アルゴリズムタイプに対応する少なくとも1つの第1アルゴリズムが直接決定される。

20

【0135】

暗号化アルゴリズムはヌル暗号化 (null encryption) アルゴリズムを含み得ることに留意されたい。ヌル暗号化アルゴリズムは、オールゼロ鍵ストリーム (all-zero keystream) を生成するために使用される。言い換えると、ヌル暗号化アルゴリズムは、情報が暗号化されていないことを示し得る。少なくとも1つの第1アルゴリズムがヌル暗号化アルゴリズムを含むとき、第1ノードと第2ノードとの間の通信情報は暗号化されないことを示す。

30

【0136】

表4から表6は、単にアルゴリズム優先度リストの例であることが理解され得る。特定の適用において、アルゴリズム優先度リストは、代替的に別の形態であってもよい。これは限定されない。

【0137】

任意に、アルゴリズムの優先度、アルゴリズムのセキュリティに関連する。例えばより高いセキュリティを有するアルゴリズムは、より高い優先度を有し、より低いセキュリティを有するアルゴリズムは、より低い優先度を有する。KDFの優先度は、KDFのセキュリティに関連する。例えば高いセキュリティを有するKDFは高い優先度を有し、低いセキュリティを有するKDFは低い優先度を有する。

40

【0138】

任意に、少なくとも1つの第1KDFは、第1ノードによってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFである。例えば少なくとも1つの第1KDFが1つのKDFを含む場合、少なくとも1つの第1KDFは、第1ノードによってサポートされ、1つ以上のKDFにおいて最も高い優先度を有するKDFである。少な

50

くとも1つの第1 K D Fがm個のK D Fを含み、mが1より大きい正の整数である場合、少なくとも1つの第1 K D Fは、第1ノードによってサポートされ、かつ1つ以上のK D Fにおいて最も高い優先度を有する第1のm個のK D Fである。

【0139】

例えば少なくとも1つの第1 K D Fは1つのK D Fを含み、第1アルゴリズムネゴシエーション要求情報は、K D F 1、K D F 2及びK D F 3を示し、K D F 1の優先度> K D F 2の優先度> K D F 3の優先度である。第1ノードによってサポートされるK D FがK D F 2及びK D F 3を含む場合、少なくとも1つの第1 K D FはK D F 2である。第1ノードによってサポートされるK D FがK D F 1及びK D F 2を含む場合、少なくとも1つの第1 K D FはK D F 1である。

【0140】

ステップ303：第1ノードは第1情報を第2ノードに送信する。

【0141】

第1情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1 K D Fを示すために使用され、その結果、第1ノードは、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1 K D Fを使用することによって第2ノードと通信する。

【0142】

任意に、少なくとも1つの第1アルゴリズムを使用することによって、完全性保護が第1情報に対して実行されるか；あるいは、少なくとも1つの第1アルゴリズムを使用することによって、第1情報が暗号化され、少なくとも1つの第1アルゴリズムを使用することによって、完全性保護が第1情報に対して実行されるか；あるいは、少なくとも1つの第1アルゴリズムを使用することによって、第1情報が暗号化される。

【0143】

少なくとも1つの第1アルゴリズムを使用することによって、完全性保護が第1情報に対して実行されるケースを最初に説明する。

【0144】

第1情報は、第2情報と第1 M A Cを含む。第2情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1 K D Fを示すために使用される。例えば第2情報は、少なくとも1つの第1アルゴリズムに関する情報及び少なくとも1つの第1 K D Fに関する情報を含む。例えば第2情報は、少なくとも1つの第1アルゴリズムの識別子及び少なくとも1つの第1 K D Fの識別子を含む。第1 M A Cは、第2情報に対して完全性保護を実行することによって取得される。

【0145】

さらに、少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズムを含み、あるいは少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズム及び暗号化アルゴリズムを含み、第1 M A Cは、完全性保護アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得され；あるいは、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、第1 M A Cは、認証された暗号化アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得される。詳細については、図6又は図7に示される以下の方法の説明を参照されたい。

【0146】

第1情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1 K D Fを以下の方式のいずれか1つで示し得る。

【0147】

方式2.1：第2情報は、第1アルゴリズムの識別子及び第1 K D Fの識別子を含む。

【0148】

例えば表3に示されるアルゴリズム／K D F識別子を例として用いる。第2情報がI D 1とI D 5を含むとき、第1情報はアルゴリズム1とK D F 2を示すために使用される。第2情報がI D 2とI D 4を含むとき、第1情報はアルゴリズム2とK D F 1を示すため

10

20

30

40

50

に使用される。

【0149】

例えばアルゴリズム／KDF識別子は表7において示され、第2情報は16ビットを含み、第1ビットから第4ビットは暗号化アルゴリズムの識別子を示すために使用され、第5ビットから第8ビットは完全性保護アルゴリズムの識別子を示すために使用され、第9ビットから第12ビットは認証された暗号化アルゴリズムの識別子を示すために使用され、第13ビットから第16ビットはKDFの識別子を示すために使用される。表7では、暗号化アルゴリズムは、アルゴリズム1、アルゴリズム2及びアルゴリズム3を含む。アルゴリズム1の識別子は0000であり、アルゴリズム1はヌル暗号化アルゴリズムであり、オールゼロ鍵ストリームを生成するために使用される。アルゴリズム2の識別子は0001であり、アルゴリズム3の識別子は0010である。完全性保護アルゴリズムは、アルゴリズム4及びアルゴリズム5を含む。アルゴリズム4の識別子は0001であり、アルゴリズム5の識別子は0010である。認証された暗号化アルゴリズムはアルゴリズム6を含み、アルゴリズム6の識別子は0011である。KDFはKDF1とKDF2を含み、KDF1の識別子は0001であり、KDF2の識別子は0010である。第2情報が0001000100000001を含む場合、第1情報は、アルゴリズム2、アルゴリズム4及びKDF1を示すために使用される。第2情報が00000000000110010を含む場合、第1情報はアルゴリズム6とKDF2を示すために使用される。

【表7】

表7

アルゴリズムタイプ	アルゴリズム／KDF	アルゴリズム／KDF識別子
暗号化アルゴリズム	アルゴリズム1	0000
	アルゴリズム2	0001
	アルゴリズム3	0010
完全性保護アルゴリズム	アルゴリズム4	0001
	アルゴリズム5	0010
認証された暗号化アルゴリズム	アルゴリズム6	0011
KDF	KDF1	0001
	KDF2	0010

【0150】

表7は、単にアルゴリズム／KDF識別子の例であることが理解され得る。特定の適用では、アルゴリズム／KDF識別子は、代替的に他の形態であってもよい。これは限定されない。

【0151】

方式2.2：第2情報は1つのビットシーケンスを含み、該ビットシーケンス内の1ビットは、1つのアルゴリズム又は1つのKDFに対応する。例えばビットシーケンス内の1ビットは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムに対応する。あるいは、ビットシーケンス内の1ビットは、第1アルゴリズムネゴシエーション要求情報によって示されるKDFに対応する。ビットシーケンスの各ビットは、0又は1を使用することによって、第1アルゴリズムがビットに対応するアルゴリズムを含むかどうか又は第1KDFがビットに対応するKDFを含むどうかを示すことができる。例えばビットが1である場合、これは、第1アルゴリズムが、そのビットに対応するアルゴリズムを含むか、あるいは第1KDFが、そのビットに対応するKDFを含むことを示すことができ、ビットが0である場合、これは、第1アルゴリズムが、そのビットに対応するアルゴリズムを含まないか、第1KDFが、そのビットに対応するKDFを

含まないことを示すことができ、逆も同様である。

【0152】

例えば第2情報は5ビットを含み、5ビット内において、第1ビットはアルゴリズム1に対応し、第2ビットはアルゴリズム2に対応し、第3ビットはアルゴリズム3に対応し、第4ビットは鍵KDF1に対応し、第5ビットは鍵KDF2に対応する。5ビットが01010である場合、これは、第1アルゴリズムがアルゴリズム2を含み、第1KDFがKDF1を含むことを示し得る。5ビットが11001である場合、これは、第1アルゴリズムがアルゴリズム1とアルゴリズム2を含み、第1KDFがKDF2を含むことを示し得る。

【0153】

方式2.3：第2情報は2つのビットシーケンスを含み、ここで、2つビットシーケンスの長さは同じであっても、異なってもよい。

【0154】

ビットシーケンスのうちの一方向のビットシーケンスについて、該ビットシーケンス内の1ビットは、1つのアルゴリズムに対応する。例えばビットシーケンス内の1ビットは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムに対応する。ビットシーケンス内の各ビットは、0又は1を使用することによって、第1アルゴリズムが、そのビットに対応するアルゴリズムを含むかどうかを示すことができる。例えばビットが1である場合、これは、第1アルゴリズムが、そのビットに対応するアルゴリズムを含むことを示すことができ、あるいはビットが0である場合、これは、第1アルゴリズムが、そのビットに対応するアルゴリズムを含まないことを示すことができ、逆も同様である。

【0155】

ビットシーケンスのうち他方のビットシーケンスについて、ビットシーケンス内の1ビットは、1つのKDFに対応する。例えばビットシーケンス内の1ビットは、第1アルゴリズムネゴシエーション要求情報によって示されるKDFに対応する。ビットシーケンス内の各ビットは、0又は1を使用することによって、第1KDFが、そのビットに対応するKDFを含むかどうかを示すことができる。例えばビットが1である場合、第1KDFが、そのビットに対応するKDFを含むことを示すことができ、ビットが0である場合、第1KDFが、そのビットに対応するKDFを含まないことを示すことができ、逆も同様である。

【0156】

例えば第2情報は2つのビットシーケンスを含み、該ビットシーケンスのうちの一方向のビットシーケンスは3ビットを含み、3ビット内の第1ビットはアルゴリズム1に対応し、3ビット内の第2ビットはアルゴリズム2に対応し、3ビット内の第3ビットはアルゴリズム3に対応し、ビットシーケンスのうち他方のビデオシーケンスは2ビットを含み、2ビット内の第1ビットは鍵KDF1に対応し、2ビット内の第2ビットは鍵KDF2に対応する。第2情報が110及び01を含む場合、これは、第1アルゴリズムがアルゴリズム1及びアルゴリズム2を含み、第1KDFがKDF2を含むことを示し得る。第2情報が010及び10を含む場合、これは、第1アルゴリズムがアルゴリズム2を含み、第1KDFがKDF1を含むことを示し得る。

【0157】

任意に、第2情報は、第1アルゴリズム又は第1KDFについての指示に関連しない情報を更に含む。例えば第2情報は、第1検証情報を更に含む。あるいは、第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含む。あるいは、第2情報は、ステップ301において、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される指示情報を更に含む。

【0158】

第1フレッシュパラメータは、第1情報の時間妥当性に関連するパラメータである。例えば第1フレッシュパラメータは、第1ノードにおけるカウンタの値又は第2ナンスを含

10

20

30

40

50

む。カウンタの値は、第1ノードのカウンタのものであり、かつ第1ノードが第1情報を送信することを決定したときに存在する値とすることができ、カウンタは、第1ノードと第2ノードとの間の通信時間の量を記録するために使用され得る。第2ナンスは、第1ノードが第1情報を送信することを決定したときに生成されるナンスであり得る。

【0159】

第1検証情報は、第1ノードによって受信された第1アルゴリズムネゴシエーション要求情報が変更されたかどうかを検証するために、第2ノードによって使用される。

【0160】

例えば第2情報は、第1検証情報を更に含む。第1検証情報は、第1ノードによって受信された第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵及び第2KDFに基づいて取得される。例えばAUTH1=第2KDF(K, 第1アルゴリズムネゴシエーション要求情報)である。ここで、AUTH1は第1検証情報である、Kはプリセット共有鍵であり、プリセット共有鍵は事前に設定される。具体的には、プリセット共有鍵は、任意の他のデバイスを使用することによって、対応するノードについて予め構成され得る。第2KDFは、第1KDFと同じであっても、異なってもよい。第2KDFが第1KDFと異なる場合、第2KDFは、第1ノード及び第2ノードにおいてプリセットされたKDFであり得る。

【0161】

例えば第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含む。第1検証情報は、第1ノードによって受信された第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵、第1フレッシュパラメータ及び第2KDFに基づいて取得される。例えばAUTH1=第2KDF(K, 第1フレッシュパラメータ, 第1アルゴリズムネゴシエーション情報)である。AUTH1、K及び第2KDFの説明については、上述の例を参照されたい。詳細は再度説明されない。

【0162】

ステップ301において、第2情報が、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される指示情報を更に含む場合、指示情報を受信した後に続いて、第2ノードは、指示情報に基づいて、第1アルゴリズムネゴシエーション要求情報内のアルゴリズム及びKDFが変更されているかどうかを決定し得ることが理解され得る。

【0163】

以下は、少なくとも1つの第1アルゴリズムを使用することによって第1情報を暗号化し、少なくとも1つの第1アルゴリズムを使用することによって第1情報に対して完全性保護を実行するケースを説明する。

【0164】

第1情報は、暗号化された情報、第2通信情報及び第2MACを含む。暗号化された情報は、第1通信情報を暗号化することによって取得され、第1通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示さない。第2通信情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFのうちの少なくとも一方を示すために使用される。第2MACは、暗号化された情報と第2通信情報に対して完全性保護を実行することによって取得される。

【0165】

さらに、少なくとも1つの第1アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み、暗号化された情報は、暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され、第2MACは、完全性保護アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することにより取得され；あるいは、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、暗号化された情報は、認証された暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され、第2MACは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することにより取得される。詳細については、図4又は図5に

示される以下の方法の説明を参照されたい。

【0166】

第1情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを以下の方式のうちのいずれか1つで示すことができる。第2通信情報は、第1アルゴリズムの識別子及び第1KDFの識別子を含み；あるいは、第2通信情報は1つのビットシーケンスを含み、該ビットシーケンス内の1ビットは、1つのアルゴリズム又は1つのKDFに対応し；あるいは、第2通信情報は2つのビットシーケンスを含み、該ビットシーケンスのうちの一方のビットシーケンスでは、該ビットシーケンス内の1ビットは、1つのアルゴリズムに対応し、ビットシーケンスのうちの他方のビットシーケンスでは、該ビットシーケンス内の1ビットは、1つのKDFに対応する。詳細については、前述の方式2.1～方式2.3における説明を参照されたい。詳細は再度説明されない。

10

【0167】

任意に、第1通信情報は、第1アルゴリズム又は第1KDFの指示に関連しない情報を含む。例えば第1通信情報は、第1検証情報を含む。あるいは、第1通信情報は、第1フレッシュパラメータ及び第1検証情報を含む。あるいは、第1通信情報は、ステップ301において1つ以上のアルゴリズムと1つ以上のKDFを示すために使用される指示情報を含む。第1検証情報、第1フレッシュパラメータ及びステップ301において1つ以上のアルゴリズムと1つ以上のKDFを示すために使用される指示情報の説明については、第2情報が、第1アルゴリズム又は第1KDFに関連しない情報を含むときに提供される前述の対応する説明を参照されたい。詳細は再度説明されない。

20

【0168】

前述の説明において、第1ノードは、最初に情報を暗号化し、次いで第2MACを取得することが理解され得る。あるいは、第1ノードは、最初に第2MACを取得し、次いで第1通信情報を暗号化し得る。これは限定されない。相違点は以下のとおりである：すなわち、第1ノードが最初に情報を暗号化し、次いで第2MACを取得するとき、第1情報を受信した後、第2ノードは第1情報の完全性を最初に検証し、第1情報の完全性を検証した後、暗号化された情報を復号する必要があることである。第1ノードが最初に第2MACを取得し、次いで第1通信情報を暗号化するとき、第1情報を受信した後、第2ノードは最初に暗号化された情報を復号し、次いで第1情報の完全性を検証する。

【0169】

以下は、少なくとも1つの第1アルゴリズムを使用することによって、第1情報が暗号化されるケースを説明する。

30

【0170】

第1情報は、暗号化された情報及び第2通信情報を含む。暗号化された情報は、第1通信情報を暗号化することによって取得される。第1通信情報及び第2通信情報の説明と、第1情報によって少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを示す説明については、少なくとも1つの第1アルゴリズムを使用することによって第1情報を暗号化し、少なくとも1つの第1アルゴリズムを使用することによって第1情報に対して完全性保護を実行する前述のケースの説明を参照されたい。詳細は再度説明されない。

【0171】

さらに、少なくとも1つの第1アルゴリズムは、暗号化アルゴリズムを含む。暗号化された情報は、暗号化アルゴリズムを使用することにより、第1通信情報を暗号化することによって取得される。例えば暗号化された情報は、暗号化鍵を使用することによって、第1通信情報を暗号化することにより取得される。暗号化鍵の説明については、図5に示される以下の方法を参照されたい。詳細は再度説明されない。

40

【0172】

少なくとも1つの第1アルゴリズムが暗号化アルゴリズムを含むケースでは、第1ノードが第2ノードと通信するとき、送信者は、暗号化鍵を使用することによって、送信されるべき情報を暗号化して、暗号化された情報を取得し、暗号化された情報を受信者に送信し得ることが理解され得る。暗号化された情報を受信した後、受信者は、暗号化鍵を使用

50

することによって、暗号化された情報を復号して、送信者の送信されるべき情報を取得し得る。このようにして、第1ノードと第2ノードと間の通信のセキュリティを向上させることができる。

【0173】

これに対応して、第2ノードは、第1ノードから第1情報を受信し得る。続いて、第2ノードは、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを使用することによって、第1ノードと通信する。

【0174】

任意に、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護が実行される場合、第2ノードは、第1情報の完全性を検証する必要がある。少なくとも1つの第1アルゴリズムを使用することによって完全性保護が第1情報に対して実行される場合、第2ノードは、第1情報を受信し、少なくとも1つの第1KDFに基づいて、認証された暗号化鍵を取得し、少なくとも1つの第1アルゴリズムと第2情報に基づいて第3MACを取得し、第3MACを使用することによって第1情報の完全性を検証する。詳細については、図6又は図7に示される以下の方法の説明を参照されたい。少なくとも1つの第1アルゴリズムを使用することによって第1情報が暗号化され、少なくとも1つの第1アルゴリズムを使用することによって第1情報に対して完全性保護が実行される場合、第2ノードは、第1情報を受信し、少なくとも1つの第1アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得し、第4MACを使用することによって第1情報の完全性を検証する。詳細については、図4又は図5に示される以下の方法の説明を参照されたい。

【0175】

任意に、第1情報を受信した後、第2ノードは、確認応答情報を第1ノードに送信する。確認応答情報は、第2ノードが第1情報を受信したことを示すために使用される。

【0176】

任意に、第1情報を受信した後、第2ノードは、第2検証情報を第1ノードに送信する。第2検証情報は、第2ノードによって受信された第1情報が変更されたかどうかを検証するために、第1ノードによって使用される。

【0177】

例えば第2検証情報は、第2ノードによって受信された第1情報、プリセット共有鍵及び第2KDFに基づいて取得される。例えばAUTH2=第2KDF(K,第1情報)である。このケースでは、第2検証情報を受信した後、第1ノードは、第1情報、プリセット共有鍵及び第2KDFに基づいて第3検証情報を取得する。例えばAUTH3=第2KDF(K,第1情報)である。第3検証情報が第2検証情報と同じである場合、これは、第2ノードによって受信された第1情報が変更されていないことを示し、第3検証情報が第2検証情報と異なる場合、これは、第2ノードによって受信された第1情報が変更されていることを示す。ここで、AUTH2は第2検証情報であり、AUTH3は第3検証情報であり、Kはプリセット共有鍵であり、第2KDFは第1KDFと同じであっても、異なってもよい。第2KDFが第1KDFと異なる場合、第2KDFは、第1ノード及び第2ノードにおいてプリセットされたKDFであり得る。

【0178】

例えば第2検証情報は、第2ノードによって受信された第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第2KDFに基づいて取得される。例えばAUTH2=第2KDF(K,第2フレッシュパラメータ,第1情報)である。このケースでは、第2検証情報を受信した後、第1ノードは、第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第2KDFに基づいて第3検証情報を取得する。例えばAUTH3=第2KDF(K,第2フレッシュパラメータ,第1情報)である。第3検証情報が第2検証情報と同じである場合、これは、第2ノードによって受信された第1情報が変更されていないことを示し；あるいは、第3検証情報が第2検証情報と異なる場合、第2ノードによって受信された第1情報が変更されていることを示す。AUTH2、AUTH3、K及び第2K

10

20

30

40

50

D Fの説明については、前述の例を参照されたい。詳細は再度説明されない。

【0179】

任意に、少なくとも1つの第1アルゴリズムを使用することによって、確認応答情報又は第2検証情報に対して完全性保護が実行される。少なくとも1つの第1アルゴリズムを使用することによって、確認応答情報又は第2検証情報に対して完全性保護を実行するプロセスについては、図4、図5、図6又は図7に示される以下の方法において、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護を実行する説明を参照されたい。詳細は再度説明されない。

【0180】

図3に示される方法に基づいて、第2ノードは、第1ノードに、1つ以上のアルゴリズム及び1つ以上のK D Fを示すために使用される第1アルゴリズムネゴシエーション要求情報を送信し得る。第1アルゴリズムネゴシエーション要求情報を受信した後、第1ノードは、第1アルゴリズムネゴシエーション要求情報に基づいて、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1K D Fを決定し、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1K D Fを示すために使用される第1情報を第2ノードに送信し得る。このようにして、第1ノードと第2ノードは、少なくとも1つの第1アルゴリズムと少なくとも1つの第1K D Fを使用することによって互いに通信してよく、これにより、第1ノードと第2ノードは、同じアルゴリズムを使用することによって、第1ノードと第2ノードとの間の通信情報を暗号化又は復号することができる。

【0181】

第1情報に含まれる内容及び／又は少なくとも1つの第1アルゴリズムに含まれ得るアルゴリズムの異なるタイプ及び数量について、いくつかの異なる実装が存在することが理解され得る。詳細については、図3に示される方法の以下の第1の実装、第2の実装、第3の実装及び第4の実装を参照されたい。

【0182】

任意に、図3に示される方法の第1の可能な実装において、第1情報は、暗号化された情報、第2通信情報及び第2M A Cを含む。少なくとも1つの第1アルゴリズムが、認証された暗号化アルゴリズムを含むとき、暗号化された情報は、認証された暗号化アルゴリズムを使用することにより第1通信情報を暗号化することによって取得され、第2M A Cは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得される。第1情報を受信した後、第2ノードは、認証された暗号化アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4M A Cを取得し、第4M A Cを使用することによって第1情報の完全性を検証し得る。具体的には、図4に示されるように、図3に示される方法は、ステップ401～ステップ404を更に含む。

【0183】

ステップ401：第1ノードは、少なくとも1つの第1K D Fに基づいて認証された暗号化鍵を取得する。

【0184】

認証された暗号化鍵は、第1通信情報を暗号化するために使用されてよく、あるいは認証された暗号化鍵は、暗号化された情報を復号するために使用されてよく、認証された暗号化鍵は、第2通信情報及び暗号化された情報に対して完全性保護を実行するために使用されてよく、あるいは認証された暗号化鍵は、第2通信情報及び暗号化された情報の完全性を検証するために使用されてもよい。

【0185】

第1ノードは、認証された暗号化鍵を以下の方式のいずれか1つで取得し得る。

【0186】

方式3. 1：第1ノードは、共有鍵を第1K D Fの入力として使用して、認証された暗号化鍵を取得する、すなわち、 $K_c = \text{第1K D F}(K)$ である、ここで、 K_c は認証された暗号化鍵であり、 K は共有鍵である。

【0187】

方式3.2：第1ノードは、共有鍵と第2フレッシュパラメータを第1KDFの入力として使用して、認証された暗号化鍵を取得する、すなわち、 $K_c = \text{第1KDF}(K, C)$ であり、ここで、 K_c は認証された暗号化鍵であり、 K は共有鍵であり、 C は第2フレッシュパラメータである。

【0188】

方式3.3：第1ノードは、共有鍵、第2フレッシュパラメータ及び第1文字列を第1KDFの入力として使用して、認証された暗号化鍵を取得する、すなわち、 $K_c = \text{第1KDF}(K, C, \text{第1文字列})$ であり、ここで、 K_c は認証された暗号化鍵であり、 K は共有鍵であり、 C は第2フレッシュパラメータである。第1文字列は、認証された暗号化アルゴリズムを識別するために使用され得る。例えば少なくとも1つの第1アルゴリズムがユーザプレーンの認証された暗号化アルゴリズムである場合、第1文字列は、ユーザプレーンの認証された暗号化アルゴリズムを識別する「user_auth_enc」であり得る。

【0189】

方式3.4：第1ノードは、共有鍵、第2フレッシュパラメータ、第1文字列及び第1識別子を第1KDFの入力として使用して、認証された暗号化鍵を取得する、すなわち、 $K_c = \text{第1KDF}(K, C, \text{第1文字列}, \text{第1識別子})$ であり、ここで、 K_c は認証された暗号化鍵であり、 K は共有鍵であり、 C は第2フレッシュパラメータである。第1文字列の説明については、前述の方式3.3を参照されたい。詳細は再度説明しない。第1識別子は、認証された暗号化鍵を生成するために使用されるKDFを識別するために使用され得る。例えば第1識別子は第1KDFの識別子であり得る。

【0190】

第1識別子は、数字及び／又は文字を含み得ることが理解され得る。方式3.4における第1文字列は、任意のパラメータであり得る。

【0191】

方式3.5：第1ノードは、共有鍵と第2フレッシュパラメータに基づいて第1中間鍵を取得し；第1ノードは第1中間鍵と、第1識別子及び第1文字列のうちの少なくとも1つに基づいて、認証された暗号化鍵を取得する。例えば第1ノードは、共有鍵と第2フレッシュパラメータをKDF1の入力として使用して、第1中間鍵を取得する、すなわち、 $K_{mid1} = \text{KDF1}(K, C)$ である。第1ノードは、第1中間鍵、第1識別子、第1文字列をKDF2の入力として使用して、認証された暗号化鍵を取得する、すなわち $K_c = \text{KDF2}(K_{mid1}, \text{第1識別子}, \text{第1文字列})$ であり、ここで、 K_{mid1} は第1中間鍵であり、 K は共有鍵であり、 C は第2フレッシュパラメータであり、 K_c は認証された暗号化鍵である。第1文字列の説明については、前述の方式3.3を参照されたい。第1識別子の説明については、前述の方式3.4の説明を参照されたい。詳細は再度説明しない。

【0192】

KDF1とKDF2は、少なくとも1つの第1KDFに含まれ得る。KDF1とKDF2は、同じであっても、異なってもよい。例えば少なくとも1つの第1KDFが1つのKDFを含む場合、KDF1とKDF2は同じである。少なくとも1つの第1KDFが2つ以上のKDFを含む場合、KDF1とKDF2は異なる。

【0193】

解決策をより明確に説明するために、認証された暗号化鍵を取得する方法は、本明細書では2つのステップで説明されることが理解され得る。実際の処理では、認証された暗号化鍵は、代替的に1つのステップで取得され得る。第1中間鍵は中間結果にすぎない。具体的には、認証された暗号化鍵を決定する方式は、 $K_c = \text{KDF2}(\text{KDF1}(K, C), \text{第1アルゴリズム}, \text{第1文字列})$ を満たす。

【0194】

任意に、前述の方式における共有鍵は、第1ノードにおいてプリセットされるか、あるいは前述の方式における共有鍵は、ステップ401の前に計算を通して第1ノードによって取得される。

【0195】

さらに、第2MACは、認証された暗号化アルゴリズム、暗号化された情報、第2通信情報及び認証された暗号化鍵に基づいて取得される。例えば第1ノードは、暗号化された情報、第2通信情報及び認証された暗号化鍵を、認証された暗号化アルゴリズムの入力として使用することによって、第2MACを取得する。

【0196】

ステップ402：第2ノードが、少なくとも1つの第1KDFに基づいて認証された暗号化鍵を取得する。

【0197】

第2ノードが、少なくとも1つの第1KDFに基づいて認証された暗号化鍵を取得する具体的なプロセスについては、第1ノードが、少なくとも1つの第1KDFに基づいて認証された暗号化鍵を取得するステップ401における対応する説明を参照されたい。詳細は再度説明しない。

10

【0198】

ステップ403：第2ノードが、認証された暗号化アルゴリズム、暗号化された情報及び第2通信情報に基づいて、第4MACを取得する。

【0199】

さらに、第2ノードは、認証された暗号化アルゴリズム、暗号化された情報、第2通信情報及び認証された暗号化鍵に基づいて第4MACを取得する。例えば第2ノードは、暗号化された情報、第2通信情報及び認証された暗号化鍵を、認証された暗号化アルゴリズムの入力として使用することによって、第4MACを取得する。

20

【0200】

第2ノードが、暗号化された情報及び第2通信情報内の一部の情報に対して完全性保護を更に実行し得ることが理解され得る。例えば第2ノードは、暗号化された情報、第2通信情報の一部の情報、認証された暗号化アルゴリズム及び認証された暗号化鍵に基づいて第4MACを取得する。

【0201】

ステップ404：第4MACが第2MACと同じである場合、第2ノードは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報を復号する。

【0202】

任意に、第4MACが第2MACと同じである場合、これは、第1通信情報が変更されていないことを示し、第2ノードは、認証された暗号化鍵を使用することによって、暗号化された情報を復号し、第1通信情報を取得する。

30

【0203】

任意に、第4MACが第2MACと異なる場合、これは、第1通信情報が変更されていることを示し、第2ノードは、第1情報を破棄する。第2ノードは、ステップ301を再度実行してもよく、あるいは第2ノードは、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを再決定するように第1ノードに指示し得る。

【0204】

第1通信情報が、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される指示情報を含むとき、第1通信情報を取得した後、第2ノードは、第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと同じであるかどうかを更に検証し得ることが理解され得る。第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと同じである場合、これは、第1アルゴリズムネゴシエーション要求情報が変更されていないことを示し、第1ノード及び第2ノードの通信環境はセキュアである。第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと異なる場合、これは、第1アルゴリズムネゴシエーション

40

50

要求情報が変更されていることを示し、第1ノード及び第2ノードの通信環境はセキュアでない。

【0205】

第1通信情報が第1検証情報を含むとき、第1通信情報を取得した後、第2ノードは、第1検証情報を使用することによって、第1アルゴリズムネゴシエーション要求情報が変更されているかどうかを検証することが理解され得る。第1アルゴリズムネゴシエーション要求情報が変更されていない場合、第1ノードと第2ノードの通信環境がセキュアであるか、あるいは第1アルゴリズムネゴシエーション要求情報が変更されている場合、第1ノードと第2ノードの通信環境はセキュアではない。

【0206】

図4に示される方法に基づいて、少なくとも1つの第1アルゴリズムが認証された暗号化アルゴリズムを含む場合、第1ノード及び第2ノードは、少なくとも1つの第1KDFに基づいて、認証された暗号化鍵を取得し得る。続いて、第1ノードは、認証された暗号化鍵を使用することによって第1通信情報を暗号化して、暗号化された情報を取得し、認証された暗号化アルゴリズム、暗号化された情報、第2通信情報及び認証された暗号化鍵に基づいて第2MACを取得し、第2MACを使用することによって、第1情報に対して完全性保護を実行し得る。第2ノードは、認証された暗号化アルゴリズム、暗号化された情報、第2通信情報及び認証された暗号化鍵に基づいて第4MACを取得し、第4MACを使用することによって第1情報の完全性を検証し得る。このようにして、第1ノードが第2ノードと通信するとき、第1通信情報は、認証された暗号化アルゴリズムを使用することによって暗号化されることができ、認証された暗号化アルゴリズムを使用することによって、完全性保護が第1情報に対して更に実行されることができ、したがって、第1ノードと第2ノードとの間の通信のセキュリティを改善することができる。

【0207】

任意に、図3に示される方法の第2の可能な実装において、第1情報は、暗号化された情報、第2通信情報及び第2MACを含む。少なくとも1つの第1アルゴリズムが暗号化アルゴリズムと完全性保護アルゴリズムを含むとき、暗号化された情報は、暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され、第2MACは、完全性保護アルゴリズムを使用することによって、暗号化された情報と第2通信情報に対して完全性保護を実行することにより取得される。第1情報を受信した後、第2ノードは、完全性保護アルゴリズム、暗号化された情報、第2通信情報に基づいて第4MACを取得し、第4MACを使用することによって第1情報の完全性を検証し得る。具体的には、図5に示されるように、図3に示される方法は、ステップ501～ステップ504を更に含む。

【0208】

ステップ501：第1ノードが、少なくとも1つの第1KDFに基づいて暗号化鍵及び完全性保護鍵を取得する。

【0209】

暗号化鍵は、第1通信情報を暗号化するために使用され得るか、あるいは暗号化鍵は、暗号化された情報を復号するために使用され得る。完全性保護鍵は、第2通信情報及び暗号化された情報に対する完全性保護を実行するために使用され得るか、あるいは完全性保護鍵は、第2通信情報及び暗号化された情報の完全性を検証するために使用され得る。

【0210】

第1ノードは、以下の方式のいずれか1つで暗号化鍵及び完全性保護鍵を取得し得る。

【0211】

方式4.1：第1ノードは、共有鍵を第1KDFの入力として使用して、暗号化鍵と完全性保護鍵を取得する、すなわち、 $K_{enc} = \text{第1KDF}(K)$ 及び $K_{int} = \text{第1KDF}(K)$ であり、ここで、 K_{enc} は暗号化鍵であり、 K は共有鍵であり、 K_{int} は完全性保護鍵である。

【0212】

方式4.2：第1ノードは、共有鍵と第2フレッシュパラメータを第1KDFの入力として使用し、暗号化鍵と完全性保護鍵を取得する、すなわち、 $K_{enc} = \text{第1KDF}(K, C)$ 及び $K_{int} = \text{第1KDF}(K, C)$ であり、ここで、 K_{enc} は暗号化鍵であり、Kは共有鍵であり、Cは第2フレッシュパラメータであり、 K_{int} は完全性保護鍵である。

【0213】

方式4.3：第1ノードは、共有鍵、第2フレッシュパラメータ及び第2文字列を第1KDFの入力として使用し、暗号化鍵を取得する、すなわち、 $K_{enc} = \text{第1KDF}(K, C, \text{第2文字列})$ である。第1ノードは、共有鍵、第2フレッシュパラメータ及び第3文字列を第1KDFの入力として使用し、完全性保護鍵を取得する、すなわち、 $K_{int} = \text{第1KDF}(K, C, \text{第3文字列})$ である。ここで、 K_{enc} は暗号化鍵であり、Kは共有鍵であり、Cは第2フレッシュパラメータであり、 K_{int} は完全性保護鍵である。第2文字列は、暗号化アルゴリズムを識別するために使用され得る。例えば少なくとも1つの第1アルゴリズムがシグナリングプレーン暗号化アルゴリズムであるとき、第2文字列は「signalling enc」であり得る。第3文字列は、完全性保護アルゴリズムを識別するために使用され得る。例えば少なくとも1つの第1アルゴリズムがシグナリングプレーン完全性保護アルゴリズムであるとき、第3文字列は「signalling int」であり得る。

【0214】

方式4.4：第1ノードは、共有鍵、第2フレッシュパラメータ、第2文字列及び第2識別子を第1KDFの入力として使用して、暗号化鍵を取得する、すなわち、 $K_{enc} = \text{第1KDF}(K, C, \text{第2文字列}, \text{第2識別子})$ である。第1ノードは、共有鍵、第2フレッシュパラメータ、第3文字列及び第3識別子を第1KDFの入力として使用し、完全性保護鍵を取得する、すなわち、 $K_{int} = \text{第1KDF}(K, C, \text{第3文字列}, \text{第3識別子})$ である。ここで、 K_{enc} は暗号化鍵であり、Kは共有鍵であり、Cは第2フレッシュパラメータであり、 K_{int} は完全性保護鍵である。第2文字列と第3文字列の説明については、上記方式3.3を参照されたい。詳細は再度説明されない。第2識別子は、暗号化鍵を生成するために使用される第1KDFを識別するために使用され得る。例えば第2識別子は、暗号化鍵を生成するために使用される第1KDFの識別子であり得る。第3識別子は、完全性保護鍵を生成するために使用されるKDFを識別するために使用され得る。例えば第3識別子は、完全性保護鍵を生成するために使用される第1KDFの識別子であり得る。

【0215】

第2識別子又は第3識別子は、数字及び／又は文字を含み得ることが理解され得る。方式4.4における第2文字列及び第3文字列は、任意のパラメータであり得る。

【0216】

方式4.5：第1ノードは、共有鍵と第2フレッシュパラメータに基づいて第2中間鍵を取得し；第1ノードは第2中間鍵と、第2識別子及び第2文字列のうちの少なくとも1つに基づいて暗号化鍵を取得する。例えば第1ノードは、共有鍵と第2フレッシュパラメータをKDF3の入力として使用して、第2中間鍵を取得する、すなわち $K_{mid2} = \text{KDF1}(K, C)$ である。第1ノードは、第2中間鍵、第2識別子及び第2文字列をKDF4の入力として使用して、暗号化鍵を取得する、すなわち、 $K_{enc} = \text{KDF2}(K_{mid2}, \text{第2識別子}, \text{第2文字列})$ である。第1ノードは、共有鍵と第2フレッシュパラメータに基づいて第3中間鍵を取得し；第1ノードは、第3中間鍵と、第3識別子及び第3文字列のうちの少なくとも1つに基づいて完全性保護鍵を取得する。例えば第1ノードは、共有鍵と第2フレッシュパラメータをKDF5の入力として使用して、第3中間鍵を取得する、すなわち、 $K_{mid3} = \text{KDF1}(K, C)$ である。第1ノードは、第3中間鍵、第3識別子及び第3文字列をKDF6の入力として使用して、完全性保護鍵を取得する、すなわち、 $K_{int} = \text{KDF2}(K_{mid3}, \text{第3識別子}, \text{第3文字列})$ である。

【0217】

ここで、 K_{mid2} は第2中間鍵であり、Kは共有鍵であり、Cは第2フレッシュパラメータであり、 K_{enc} は暗号化鍵であり、 K_{mid3} は第3中間鍵であり、 K_{int} は完全

性保護鍵である。第2文字列及び第3文字列の説明については、前述の方式4.3を参照されたい。第2識別子及び第3識別子の説明については、前述の方式4.4の説明を参照されたい。詳細は再度説明されない。

【0218】

KDF3、KDF4、KDF5及びKDF6は、少なくとも1つの第1KDFに含まれる。KDF3とKDF4は、同じであっても、異なってもよい。KDF5とKDF6は、同じであっても、異なってもよい。

【0219】

解決策をより明確に説明するために、暗号化鍵及び完全性保護鍵を取得する方法は、本明細書では2つのステップで説明されることが理解され得る。実際の処理では、暗号化鍵と完全性保護鍵は、代替的に1つのステップで取得されてもよい。第2中間鍵及び第3中間鍵は単なる中間結果である。具体的には、暗号化鍵を決定する方式は、 $K_{enc} = KDF4(KDF3(K, C), 第2アルゴリズム, 第2文字列)$ を満たし、完全性保護鍵を決定する方式は、 $K_{int} = KDF6(KDF5(K, C), 第3アルゴリズム, 第3文字列)$ を満たす。

【0220】

任意に、前述の方式における共有鍵は、第1ノードにおいてプリセットされるか、あるいは前述の方式における共有鍵は、ステップ501の前の計算を通して第1ノードによって取得される。

【0221】

任意に、前述の方式において、暗号化鍵を生成するための第1KDFは、完全性保護鍵を生成するための第1KDFと同じであるか又は異なる。例えば少なくとも1つの第1KDFは1つのKDFを含み、暗号化鍵を生成する第1KDFは、完全性保護鍵を生成するための第1KDFと同じであるか；あるいは、少なくとも1つの第1KDFは複数のKDFを含み、暗号化鍵を生成するための第1KDFは、完全性保護鍵を生成するための第1KDFとは異なる。

【0222】

さらに、第2MACは、完全性保護アルゴリズム、暗号化された情報、第2通信情報及び完全性保護鍵に基づいて取得される。例えば第1ノードは、暗号化された情報、第2通信情報及び完全性保護鍵を完全性保護アルゴリズムの入力として使用することによって、第2MACを取得する。

【0223】

ステップ502：第2ノードが、少なくとも1つの第1KDFに基づいて暗号化鍵と完全性保護鍵を取得する。

【0224】

第2ノードが少なくとも1つの第1KDFに基づいて暗号化鍵と完全性保護鍵を取得する具体的なプロセスについては、第1ノードが少なくとも1つの第1KDFに基づいて暗号化鍵と完全性保護鍵を取得するステップ501の対応する説明を参照されたい。詳細は再度説明されない。

【0225】

ステップ503：第2ノードは、完全性保護アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得する。

【0226】

さらに、第2ノードは、完全性保護アルゴリズム、暗号化された情報、第2通信情報及び完全性保護鍵に基づいて第4MACを取得する。例えば第2ノードは、暗号化された情報、第2通信情報及び完全性保護鍵を完全性保護アルゴリズムの入力として使用することによって、第4MACを取得する。

【0227】

第2ノードは、暗号化された情報と、第2通信情報内の一部の情報に対して完全性保護を更に実行し得ることが理解され得る。例えば第2ノードは、暗号化された情報、第2通

10

20

30

40

50

信情報内の一部の情報、完全性保護アルゴリズム及び完全性保護鍵に基づいて第4MACを取得する。

【0228】

ステップ504：第4MACが第2MACと同じである場合、第2ノードは、暗号化アルゴリズムを使用することによって、暗号化された情報を復号する。

【0229】

任意に、第4MACが第2MACと同じである場合、これは、第1通信情報が変更されていないことを示し、第2ノードは、暗号化鍵を使用することによって暗号化された情報を復号して、第1通信情報を取得する。

【0230】

任意に、第4MACが第2MACと異なる場合、これは、第1通信情報が変更されていることを示し、第2ノードは第1情報を破棄する。第2ノードは、ステップ301を再度実行してもよく、あるいは第2ノードは、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを再決定するように第1ノードに指示し得る。

【0231】

第1通信情報が、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される指示情報を含むとき、第1通信情報を取得した後、第2ノードは、第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと同じであるかどうかを更に検証し得ることが理解され得る。第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと同じである場合、これは、第1アルゴリズムネゴシエーション要求情報が変更されていないことを示し、第1ノードと第2ノードの通信環境はセキュアである。第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFとは異なる場合、これは、第1アルゴリズムネゴシエーション要求情報が変更されていることを示し、第1ノードと第2ノードの通信環境はセキュアではない。

【0232】

第1通信情報が第1検証情報を含むとき、第1通信情報を取得した後、第2ノードは、第1検証情報を使用することによって、第1アルゴリズムネゴシエーション要求情報が変更されているかどうかを検証することが理解され得る。第1アルゴリズムネゴシエーション要求情報が変更されていない場合、第1ノードと第2ノードの通信環境はセキュアであり；あるいは、第1アルゴリズムネゴシエーション要求情報が変更されている場合、第1ノードと第2ノードの通信環境はセキュアではない。

【0233】

図5に示される方法に基づいて、少なくとも1つの第1アルゴリズムが、暗号化アルゴリズムと完全性保護アルゴリズムを含むとき、第1ノードと第2ノードは、少なくとも1つの第1KDFに基づいて、暗号化鍵と完全性保護鍵を取得し得る。続いて、第1ノードは、暗号化鍵を使用することによって第1通信情報を暗号化して、暗号化された情報を取得し、完全性保護アルゴリズム、暗号化された情報、第2通信情報及び完全性保護鍵に基づいて第2MACを取得し、第2MACを使用することによって第1通信情報に対して完全性保護を実行し得る。第2ノードは、完全性保護アルゴリズム、暗号化された情報、第2通信情報及び完全性保護鍵に基づいて第4MACを取得し、第4MACを使用することによって第1情報の完全性を検証し得る。このようにして、第1ノードが第2ノードと通信するとき、第1通信情報は、暗号化アルゴリズムを使用することによって暗号化されることができ、完全性保護アルゴリズムを使用することによって、完全性保護を第1情報に対して更に実行することができる。したがって、第1ノードと第2ノードとの間の通信のセキュリティを改善することができる。

【0234】

任意に、図3に示される方法の第3の可能な実装では、第1情報は第2情報及び第1MACを含む。少なくとも1つの第1アルゴリズムが暗号化アルゴリズムと完全性保護アルゴリズムを含むとき、第1MACは、完全性保護アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することによって取得される。第1情報を受信した後、第2ノードは、完全性保護アルゴリズム、第2情報及び完全性保護鍵に基づいて第3MACを取得し、第3MACを使用することによって第1情報の完全性を検証し得る。具体的には、図6に示されるように、図3に示される方法は、ステップ601～ステップ603を更に含む。

【0235】

ステップ601：第1ノードは、少なくとも1つの第1KDFに基づいて完全性保護鍵を取得する。

10

【0236】

ステップ601の具体的なプロセスについては、ステップ501における対応する説明を参照されたい。詳細は再度説明されない。

【0237】

さらに、第1MACが、完全性保護アルゴリズム、第2情報及び完全性保護鍵に基づいて取得される。例えば第1ノードは、第2情報及び完全性保護鍵を完全性保護アルゴリズムの入力として使用することによって、第1MACを取得する。

【0238】

任意に、第1ノードは、少なくとも1つの第1KDFに基づいて暗号化鍵を取得し、それにより、第1ノードと第2ノードは、その後、暗号化鍵を使用することによって、第1ノードと第2ノードとの間の通信情報を暗号化又は復号する。これは、第1ノードと第2ノードとの間の通信のセキュリティが改善する。第1ノードが少なくとも1つの第1KDFに基づいて暗号化鍵を取得するプロセスについては、ステップ501における対応する説明を参照されたい。詳細は、再度説明しない。

20

【0239】

ステップ602：第2ノードは、少なくとも1つの第1KDFに基づいて完全性保護鍵を取得する。

【0240】

ステップ602の具体的なプロセスについては、ステップ502における対応する説明を参照されたい。詳細は再度説明されない。

30

【0241】

任意に、第2ノードは、少なくとも1つのKDFに基づいて暗号化鍵を取得する。第2ノードが少なくとも1つの第1KDFに基づいて暗号化鍵を取得するプロセスについては、ステップ502における対応する説明を参照されたい。詳細は、再度説明しない。

【0242】

ステップ603：第2ノードは、完全性保護アルゴリズム及び第2情報に基づいて第3MACを取得する。

【0243】

第3MACは、第2情報の完全性を検証するために使用され得る。

40

【0244】

さらに、第2ノードは、完全性保護アルゴリズム、第2情報及び完全性保護鍵に基づいて第3MACを取得する。例えば第2ノードは、第2情報と完全性保護鍵を完全性保護アルゴリズムの入力として使用することによって、第3MACを取得する。

【0245】

第2ノードは、第2情報内の一部の情報に対して完全性保護を更に実行し得ることが理解され得る。例えば第2ノードは、第2情報内の一部の情報、完全性保護アルゴリズム及び完全性保護鍵に基づいて第3MACを取得する。

【0246】

第3MACが第1MACと同じである場合、これは、第2情報が変更されていないこと

50

を示し、第2ノードと第1ノードは、少なくとも1つの第1アルゴリズムと少なくとも1つの第1KDFを使用することによって、互いに通信することができることに留意されたい。第3MACが第1MACと異なる場合、これは、第1情報が変更されていることを示し、第2ノードは、ステップ301を再度実行し得るか；あるいは第2ノードは、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを再決定するように第1ノードに指示し得る。

【0247】

第1通信情報が、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される指示情報を含むとき、第1通信情報を取得した後、第2ノードは、第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと同じであるかどうかを更に検証し得るが理解され得る。第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFと同じである場合、これは、第1アルゴリズムネゴシエーション要求情報が変更されていないことを示し、第1ノードと第2ノードの通信環境はセキュアである。第1通信情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFが、第1アルゴリズムネゴシエーション要求情報に含まれる1つ以上のアルゴリズム及び1つ以上のKDFとは異なる場合、これは、第1アルゴリズムネゴシエーション要求情報が変更されていることを示し、第1ノードと第2ノードの通信環境がセキュアではない。

【0248】

第1通信情報が第1検証情報を含む場合、第1通信情報を取得した後、第2ノードは、第1検証情報を使用することによって、第1アルゴリズムネゴシエーション要求情報が変更されているかどうかを検証することが理解され得る。第1アルゴリズムネゴシエーション要求情報が変更されていない場合、第1ノードと第2ノードの通信環境はセキュアであり；あるいは、第1アルゴリズムネゴシエーション要求情報が変更されている場合、第1ノードと第2ノードの通信環境はセキュアではない。

【0249】

図6に示される方法に基づいて、少なくとも1つの第1アルゴリズムが暗号化アルゴリズム及び完全性保護アルゴリズムを含むとき、第1ノードと第2ノードは、少なくとも1つの第1KDFに基づいて暗号化鍵及び完全性保護鍵を取得し得る。続いて、第1ノードは、完全性保護アルゴリズム、第2情報及び完全性保護鍵に基づいて第1MACを取得し、第1MACを使用することによって、第1情報に対して完全性保護を実行し得る。第2ノードは、完全性保護アルゴリズム、第2情報及び完全性保護鍵に基づいて第3MACを取得し、第3MACを使用することによって、第1情報の完全性を検証し得る。このようにして、第1ノードが第2ノードと通信するとき、完全性保護アルゴリズムを使用することによって、第1情報に対して完全性保護を実行することができる。したがって、第1ノードと第2ノードとの間の通信のセキュリティを改善することができる。

【0250】

任意に、図3に示される方法の第4の可能な実装において、第1情報は、第2情報及び第1MACを含む。少なくとも1つの第1アルゴリズムが認証された暗号化アルゴリズムを含むとき、第1MACは、認証された暗号化アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得される。第1情報を受信した後、第2ノードは、認証された暗号化アルゴリズム、第2情報及び認証された暗号化鍵に基づいて第3MACを取得し、第3MACを使用することによって、第1情報の完全性を検証し得る。具体的には、図7に示されるように、図3に示される方法は、ステップ701～ステップ703を更に含む。

【0251】

ステップ701：第1ノードは、少なくとも1つの第1KDFに基づいて認証された暗号化鍵を取得する。

【0252】

ステップ701の具体的なプロセスについては、ステップ401における対応する説明を参照されたい。詳細は再度説明されない。

【0253】

さらに、第1MACは、認証された暗号化アルゴリズム、第2情報及び認証された暗号化鍵に基づいて取得される。例えば第1ノードは、第2情報と認証された暗号化鍵を認証された暗号化アルゴリズムの入力として使用することによって、第1MACを取得する。

【0254】

ステップ702：第2ノードは、少なくとも1つの第1KDFに基づいて認証された暗号化鍵を取得する。

10

【0255】

ステップ702の具体的なプロセスについては、ステップ402における対応する説明を参照されたい。詳細は再度説明されない。

【0256】

ステップ703：第2ノードは、認証された暗号化アルゴリズム及び第2情報に基づいて第3MACを取得する。

【0257】

第3MACは、第2情報の完全性を検証するために使用され得る。

【0258】

さらに、第2ノードは、認証された暗号化アルゴリズム、第2情報及び認証された暗号化鍵に基づいて第3MACを取得する。例えば第2ノードは、第2情報と認証された暗号化鍵を、認証された暗号化アルゴリズムの入力として使用することによって第3MACを取得する。

20

【0259】

第2ノードが、第2情報内の一部の情報に対して完全性保護を実行し得ることが理解され得る。例えば第2ノードは、第2情報内の一部の情報、認証された暗号化アルゴリズム及び認証された暗号化鍵に基づいて第3MACを取得する。

【0260】

第3MACが第1MACと同じである場合、これは、第2情報が変更されていないことを示し、第2ノードと第1ノードは、少なくとも1つの第1KDFと少なくとも1つの第1KDFを使用することによって、互いに通信し得ることに留意されたい。第3MACが第1MACと異なる場合、これは、第1情報が変更されていないことを示し、第2ノードは、ステップ301を再度実行してよく、あるいは第2ノードは、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを再決定するように第1ノードに指示し得る。

30

【0261】

第1通信情報が、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される指示情報を含むケース及び第1通信情報が第1検証情報を含むケースについては、図6における方法の説明を参照することが理解され得る。詳細は再度説明されない。

【0262】

40

図7に示される方法に基づいて、少なくとも1つの第1アルゴリズムが、認証された暗号化アルゴリズムを含むとき、第1ノード及び第2ノードは、少なくとも1つの第1KDFに基づいて、認証された暗号化鍵を取得し得る。続いて、第1ノードは、認証された暗号化アルゴリズム、第2情報及び認証された暗号化鍵に基づいて第1MACを取得し、第1MACを使用することによって、第1情報に対して完全性保護を実行し得る。第2ノードは、認証された暗号化アルゴリズム、第2情報及び認証された暗号化鍵に基づいて第3MACを取得し、第3MACを使用することによって、第1情報の完全性を検証し得る。このようにして、第1ノードが第2ノードと通信するとき、認証された暗号化アルゴリズムを使用することによって、完全性保護が第1情報に対して実行され得る。したがって、第1ノードと第2ノードとの間の通信のセキュリティを改善することができる。

50

【0263】

図3に示される方法、図4に示される方法、図5に示される方法又は図6に示される方法のステップ301の前に、第2ノードは、1つ以上のアルゴリズム及び1つ以上のKDFの指示情報を第1ノードに複数回送信してよく、その結果、第1ノードは、複数回送信された指示情報から少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを決定することが理解され得る。以下は、図3に示される方法を例として用いて、上述のプロセスを説明する。

【0264】

任意に、図8に示されるように、図3に示される方法の第5の可能な実装において、図3に示される方法は、ステップ801及びステップ802を更に含む。

【0265】

ステップ801：第2ノードは、第2アルゴリズムネゴシエーション要求情報を第1ノードに送信する。

【0266】

第2アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用され得る。

【0267】

任意に、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムとは異なる。例えば第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムとは完全に異なる。あるいは、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムと完全には同じではない。第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFとは異なる。例えば第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFとは完全に異なる。あるいは、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFと完全には同じではない。

【0268】

任意に、第2アルゴリズムネゴシエーション要求情報は、第2ノードの識別子及び第3フレッシュパラメータを更に含む。第2ノードの識別子は、第2ノードを識別するために使用され得る。第3フレッシュパラメータは、第2アルゴリズムネゴシエーション要求情報の時間妥当性に関連するパラメータである。例えば第3フレッシュパラメータは、第2ノードにおけるカウンタの値又は第3ナンスを含む。カウンタの値は、第2ノードのカウンタのものであり、かつ第2ノードが第2アルゴリズムネゴシエーション要求情報を送信することを決定したときに存在する値とすることができ、カウンタは、第1ノードと第2ノードとの間の通信時間の量を記録するために使用され得る。第3ナンスは、第2ノードが第2アルゴリズムネゴシエーション要求情報を送信することを決定したときに、第2ノードによって生成されるナンスであり得る。

【0269】

ステップ801の具体的なプロセスについては、第2ノードが第1アルゴリズムネゴシエーション要求情報を第1ノードに送信するステップ301の対応する説明を参照されたい。詳細は再度説明されない。

【0270】

ステップ802：第1ノードは、第2ノードから第2アルゴリズムネゴシエーション要求情報を受信し、第3情報を第2ノードに送信する。

【0271】

第3情報は、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFが、サポートされていないか又は適用可能でないことを示すために使用され得る。

【0272】

第1ノードが、第2ノードによって示される1つ以上のアルゴリズム及び1つ以上のKDFがサポートされていないか又は適用可能でないことを示すとき、第1ノードが、第2ノードによって示される1つ以上のアルゴリズム及び1つ以上のKDFに基づいて少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを決定するまで、第2ノードはステップ801を再度実行し得ることが理解され得る。

【0273】

図3に示される方法のステップ301の前に実行されることに加えて、ステップ801及びステップ802は、図4、図5、図6又は図7に示される方法のステップ301の前に実行されてもよいことが理解され得る。これは限定されない。

【0274】

図8に示される方法に基づいて、第1ノードが少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを決定する前に、第2ノードは、1つ以上のアルゴリズム及び1つ以上のKDFの指示情報を第1ノードに複数回送信し得る。このようにして、第2ノードは、1つ以上のアルゴリズム及び1つ以上のKDFの指示情報を第1ノードに複数回送信することによって、第1ノードと第2ノードとの間で使用されるアルゴリズム及びKDFについて第1ノードとネゴシエーションすることができる。

【0275】

本出願の実施態様において提供される解決策は、主に、第1ノードと第2ノードとの間の対話の観点から上記で説明されている。前述の機能を実装するために、第1ノード又は第2ノードは、機能を実行するために対応するハードウェア構造及び／又はソフトウェアモジュールを含むことが理解され得る。当業者は、本明細書で開示される実施形態で説明されるユニット及びアルゴリズム操作の例と組み合わせて、本出願を、ハードウェア又はハードウェアとコンピュータソフトウェアの組合せによって実装することができることに容易に気づくべきである。機能がハードウェアによって実行されるか又はコンピュータソフトウェアにより駆動されるハードウェアによって実行されるかは、特定の適用と技術的解決策の設計的制約に依存する。当業者は、特定の用途ごとに、異なる方法を使用して説明された機能を実装することができ、その実装が本出願の範囲を超えるものと見なされるべきではない。

【0276】

本出願の実施形態では、第1ノード又は第2ノードは、前述の方法例に基づいて機能モジュールに分割され得る。例えば各機能モジュールは、各対応する機能に基づく分割を通して取得されてもよく、あるいは2つ以上の機能が1つの処理モジュールに統合されてもよい。統合モジュールは、ハードウェアの形態で実装され得るか又はソフトウェア機能モジュールの形態で実装され得る。本出願の実施態様において、モジュールへの分割は一例であり、単に論理機能分割であることに留意されたい。実際の実装の間に、別の分割方式が存在してもよい。

【0277】

例えば各機能モジュールが統合方式の分割を通して取得されるとき、図9は通信装置の概略構造図である。通信装置は、第1ノードであるか又は第1ノード内のチップ又はシステムオンチップであってよく、通信装置は、前述の実施形態における第1ノードの機能を実行するよう構成され得る。

【0278】

可能な実施形態では、図9に示される通信装置は、受信モジュール901、処理モジュール902及び送信モジュール903を含む。

【0279】

受信モジュール901は、第1アルゴリズムネゴシエーション要求情報を第2ノードか

10

20

30

40

50

ら受信するよう構成され、ここで、第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される。

【0280】

処理モジュール902は、1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、1つ以上のKDFにおける少なくとも1つの第1KDFを決定するよう構成される。

【0281】

送信モジュール903は、第1情報を第2ノードに送信するよう構成され、ここで、第1情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを示すために使用される。

【0282】

任意に、1つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む。

【0283】

任意に、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護が実行される。

【0284】

任意に、第1情報は、第2情報及び第1メッセージ認証コードMACを含み、第2情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを示すために使用され、第1MACは、第2情報に対して完全性保護を実行することによって取得される。

【0285】

任意に、少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズムを含み、第1MACは、完全性保護アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得されるか；あるいは、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、第1MACは、認証された暗号化アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得される。

【0286】

任意に、第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含み、第1フレッシュパラメータは、第1情報の時間妥当性に関連するパラメータであり、第1検証情報は、第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵、第1フレッシュパラメータ及び第1KDFに基づいて取得される。

【0287】

任意に、第1情報は、暗号化された情報、第2通信情報及び第2メッセージ認証コードMACを含み；暗号化された情報は、第1通信情報を暗号化することによって取得され、第1通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示さず、第2通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示すために使用され；第2MACは、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得される。

【0288】

任意に、少なくとも1つの第1アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み；暗号化された情報は、暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、完全性保護アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得される。

【0289】

任意に、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み；暗号化された情報は、認証された暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報及び第2通信情報の完全性保護を実行するこ

10

20

30

40

50

とにより取得される。

【0290】

任意に、少なくとも1つの第1アルゴリズムは、通信装置によってサポートされ、かつ1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、少なくとも1つの第1KDFは、通信装置によってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFである。

【0291】

任意に、第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを更に含み、第2フレッシュパラメータは、第1アルゴリズムネゴシエーション要求情報の時間妥当性に関連するパラメータであり；受信モジュール901は、第2ノードから第2検証情報を受信するよう更に構成され、ここで、第2検証情報は、第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて取得され；処理モジュール902は、第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて第2検証情報を検証するよう更に構成される。

10

【0292】

任意に、受信モジュール901は、第2アルゴリズムネゴシエーション要求情報を第2ノードから受信するよう更に構成され、ここで、第2アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用され；送信モジュール903は、第3情報を第2ノードに送信するよう更に構成され、ここで、第3情報は、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFがサポートされていないか又は適用可能でないことを示すために使用される。

20

【0293】

任意に、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムとは異なり；第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFとは異なる。

【0294】

前述の方法の実施形態における動作のすべての関連する内容は、対応する機能モジュールの機能説明において引用され得る。詳細はここでは説明されない。

30

【0295】

この実施形態では、通信装置は、分割を通して取得される機能モジュールの統合方式の形態で提示される。本明細書において「モジュール」は、特定のASIC、回路、1つ以上のソフトウェア又はファームウェアプログラムを実行するプロセッサとメモリ、集積論理回路及び／又は前述の機能を提供することができる別の構成要素であり得る。単純な実施形態では、当業者は、通信装置が図2に示される形態であり得ることを理解し得る。

【0296】

例えば図2のプロセッサ201は、メモリ203に記憶されたコンピュータ実行可能命令を呼び出して、通信装置が前述の方法の実施形態における通信方法を実行することを可能にし得る。

40

【0297】

例えば図9の受信モジュール901、処理モジュール902及び送信モジュール903の機能／実装プロセスは、メモリ203に記憶されたコンピュータ実行可能命令を呼び出すことによって、図2のプロセッサ201によって実装され得る。あるいは、図9の処理モジュール902の機能／実装プロセスは、メモリ203に記憶されたコンピュータ実行可能命令を呼び出すことによって、図2のプロセッサ201によって実装されてよく、図9の受信モジュール901及び送信モジュール903の機能／実装プロセスは、図2の通信インタフェース204によって実装されてもよい。

【0298】

50

この実施形態で提供される通信装置は、前述の通信方法を実行するよう構成され得る。したがって、通信装置によって達成することができる技術的效果については、前述の方法の実施形態を参照されたい。詳細はここでは説明されない。

【0299】

例えば各機能モジュールが統合方式で分割を通して取得されるとき、図10は通信装置の概略構造図である。通信装置は、第2ノードであるか又は第2ノード内のチップ又はシステムオンチップであってよく、通信装置は、前述の実施形態における第2ノードの機能を実行するよう構成され得る。

【0300】

可能な実施形態では、図10に示される通信装置は、送信モジュール1001及び受信モジュール1002を含む。

【0301】

送信モジュール1001は、第1アルゴリズムネゴシエーション要求情報を第1ノードに送信するよう構成され、ここで、第1アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用される。

【0302】

受信モジュール1002は、第1ノードから第1情報を受信するよう構成され、ここで、第1情報は、1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、1つ以上のKDFにおける少なくとも1つの第1KDFを示すために使用される。

【0303】

任意に、1つ以上のアルゴリズムは、暗号化アルゴリズム及び／又は完全性保護アルゴリズム及び／又は認証された暗号化アルゴリズムを含む。

【0304】

任意に、少なくとも1つの第1アルゴリズムを使用することによって、第1情報に対して完全性保護が実行される。

【0305】

任意に、第1情報は、第2情報と第1メッセージ認証コードMACを含み、第2情報は、少なくとも1つの第1アルゴリズム及び少なくとも1つの第1KDFを示すために使用され、第1MACは、第2情報に対して完全性保護を実行することによって取得される。

【0306】

任意に、図11に示されるように、通信装置は、処理モジュール1003を更に含み；少なくとも1つの第1アルゴリズムは、完全性保護アルゴリズムを含み、第1MACは、完全性保護アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得され、処理モジュール1003は、完全性保護アルゴリズム及び第2情報に基づいて第3MACを取得するよう構成され、ここで、第3MACは、第2情報の完全性を検証するために使用され；あるいは、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、第1MACは、認証された暗号化アルゴリズムを使用することによって、第2情報に対して完全性保護を実行することにより取得され、処理モジュール1003は、認証された暗号化アルゴリズム及び第2情報に基づいて第3MACを取得するよう構成され、ここで、第3MACは、第2情報の完全性を検証するために使用される。

【0307】

任意に、第2情報は、第1フレッシュパラメータ及び第1検証情報を更に含み、第1フレッシュパラメータは、第1情報の時間妥当性に関連するパラメータであり、第1検証情報は、第1アルゴリズムネゴシエーション要求情報、プリセット共有鍵、第1フレッシュパラメータ及び第1KDFに基づいて取得される。

【0308】

任意に、第1情報は、暗号化された情報、第2通信情報及び第2メッセージ認証コードMACを含み；暗号化された情報は、第1通信情報を暗号化することによって取得され、第1通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFの

10

20

30

40

50

うちの少なくとも一方を示さず、第2通信情報は、少なくとも1つの第1アルゴリズム又は少なくとも1つの第1KDFのうちの少なくとも一方を示すために使用され；第2MACは、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得される。

【0309】

任意に、少なくとも1つの第1アルゴリズムは、暗号化アルゴリズム及び完全性保護アルゴリズムを含み、暗号化された情報は、暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、完全性保護アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することによって取得され；処理モジュール1003は、完全性保護アルゴリズム、暗号化された情報及び第2通信情報に基づいて第4MACを取得するよう構成され；処理モジュール1003は、第4MACが第2MACと同じである場合、暗号化アルゴリズムを使用することによって暗号化された情報を復号するように更に構成される。

10

【0310】

任意に、少なくとも1つの第1アルゴリズムは、認証された暗号化アルゴリズムを含み、暗号化された情報は、認証された暗号化アルゴリズムを使用することによって、第1通信情報を暗号化することにより取得され；第2MACは、認証された暗号化アルゴリズムを使用することによって、暗号化された情報及び第2通信情報に対して完全性保護を実行することにより取得され、処理モジュール1003は、認証された暗号化アルゴリズム、暗号化された情報及び第2通信情報に基づいて、第4MACを取得するよう構成され；処理モジュール1003は、第4MACが第2MACと同じである場合、認証された暗号化アルゴリズムを使用することによって、暗号化された情報を復号するように更に構成される。

20

【0311】

任意に、少なくとも1つの第1アルゴリズムは、第1ノードによってサポートされ、かつ1つ以上のアルゴリズムにおいて最も高い優先度を有するアルゴリズムであり、少なくとも1つの第1KDFは、第1ノードによってサポートされ、かつ1つ以上のKDFにおいて最も高い優先度を有するKDFである。

【0312】

任意に、第1アルゴリズムネゴシエーション要求情報は、第2フレッシュパラメータを更に含み、第2フレッシュパラメータは、第1アルゴリズムネゴシエーション要求情報の時間妥当性に関連するパラメータであり、送信モジュール1001は、第2検証情報を第1ノードに送信するよう更に構成され、ここで、第2検証情報は、第1情報、プリセット共有鍵、第2フレッシュパラメータ及び第1KDFに基づいて取得される。

30

【0313】

任意に、送信モジュール1001は、第2アルゴリズムネゴシエーション要求情報を第1ノードに送信するよう更に構成され、ここで、第2アルゴリズムネゴシエーション要求情報は、1つ以上のアルゴリズム及び1つ以上のKDFを示すために使用され；受信モジュール1002は、第1ノードから第3情報を受信するよう更に構成され、ここで、第3情報は、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズム及び1つ以上のKDFが、サポートされていないか又は適用可能でないことを示すために使用される。

40

【0314】

任意に、第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のアルゴリズムとは異なり；第2アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFは、第1アルゴリズムネゴシエーション要求情報によって示される1つ以上のKDFとは異なる。

【0315】

前述の方法の実施形態における動作のすべての関連する内容は、対応する機能モジュール

50

ルの機能説明において引用され得る。詳細はここでは説明されない。

【0316】

この実施形態では、通信装置は、分割を通して取得される機能モジュールの統合方式の形態で提示される。本明細書において「モジュール」は、特定のASIC、回路、1つ以上のソフトウェア又はファームウェアプログラムを実行するプロセッサとメモリ、集積論理回路及び／又は前述の機能を提供することができる別の構成要素であり得る。単純な実施形態では、当業者は、通信装置が図2に示される形態であり得ることを理解し得る。

【0317】

例えば図2のプロセッサ201は、メモリ203に記憶されたコンピュータ実行可能命令を呼び出して、通信装置が前述の方法の実施形態における通信方法を実行することを可能にし得る。

10

【0318】

例えば図11の送信モジュール1001、受信モジュール1002及び処理モジュール1003の機能／実装プロセスは、メモリ203に記憶されたコンピュータ実行可能命令を呼び出すことによって、図2のプロセッサ201によって実装され得る。あるいは、図11の処理モジュール1003の機能／実装プロセスは、メモリ203に記憶されたコンピュータ実行可能命令を呼び出すことによって、図2のプロセッサ201によって実装されてもよく、図11の送信モジュール1001及び受信モジュール1002の機能／実装プロセスは、図2の通信インタフェース204によって実装されてもよい。

【0319】

20

この実施形態で提供される通信装置は、前述の通信方法を実行するよう構成され得る。したがって、通信装置によって達成することができる技術的效果については、前述の方法の実施形態を参照されたい。詳細はここでは説明されない。

【0320】

図12は、通信システムの概略構成図である。図12に示されるように、通信システム120は、ノード1201及びノード1202を含み得る。図12は、単に例示的な添付図面であり、図12に示される通信システム120に含まれるノード及びノードの数量は、本出願のこの実施形態において限定されないことに留意されたい。

【0321】

ノード1201は、図9に示される通信装置の機能を有し、第1アルゴリズムネゴシエーション要求情報を第2ノードから受信し、1つ以上のアルゴリズムにおける少なくとも1つの第1アルゴリズムと、1つ以上のKDFにおける少なくとも1つの第1KDFを決定し、第1情報を第2ノードに送信するよう構成される。

30

【0322】

ノード1202は、図10又は図11に示される通信装置の機能を有し、第1アルゴリズムネゴシエーション要求情報を第1ノードに送信し、第1情報を第1ノードから受信するよう構成され得る。

【0323】

前述の方法の実施形態におけるステップのすべての関連する内容は、通信システム120の対応するノードの機能説明において引用され得ることに留意されたい。詳細はここでは説明されない。

40

【0324】

図13は、本出願の一実施形態によるチップの概略構造図である。チップ130は、1つ以上のプロセッサ1301及びインタフェース回路1302を含む。任意に、チップ130は、バス1303を更に含む得る。

【0325】

プロセッサ1301は、集積回路チップであってよく、信号処理能力を有する。実装プロセスにおいて、前述の方法におけるステップは、プロセッサ1301内のハードウェア集積論理回路を使用することによって又はソフトウェアの形式の命令を使用することによって実装され得る。プロセッサ1301は、汎用プロセッサ、デジタル信号プロセッサ（

50

DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)又は別のプログラマブルロジックデバイス、離散ゲート又はトランジスタ論理デバイス、あるいは離散ハードウェア構成要素であり得る。プロセッサは、本出願の実施形態において開示される方法及びステップを実装又は実行し得る。汎用プロセッサは、マイクロプロセッサであってよく、あるいはプロセッサは、任意の従来のプロセッサ等であってよい。

【0326】

インタフェース回路1302は、データ、命令又は情報を送信又は受信するよう構成される。プロセッサ1301は、インタフェース回路1302によって受信されるデータ、命令又は他の情報を使用することによって処理を実行してよく、インタフェース回路1302を使用することによって処理された情報を送信し得る。

10

【0327】

任意に、チップ130はメモリを更に含む。メモリは、読取専用メモリ及びランダムアクセスメモリを含んでよく、プロセッサのための操作命令及びデータを提供し得る。メモリの一部は、不揮発性ランダムアクセスメモリ(NVRAM)を更に含み得る。

【0328】

任意に、メモリは、実行可能ソフトウェアモジュール又はデータ構造を記憶し、プロセッサは、メモリに記憶された動作命令(動作命令は、オペレーティングシステムに記憶され得る)を呼び出すことによって対応する動作を実行し得る。

20

【0329】

任意に、チップ130は、本出願の実施形態における通信装置(第1ノード及び第2ノードを含む)において使用され得る。任意に、インタフェース回路1302は、プロセッサ1301の実行結果を出力するよう構成され得る。本出願の1つ以上の実施形態において提供される通信方法については、前述の実施形態を参照されたい。詳細は、ここでは再度説明されない。

【0330】

プロセッサ1301及びインタフェース回路1302に対応する機能は、ハードウェア設計を使用することによって実装されてよく、あるいはソフトウェア設計を使用して実装されてもよく、あるいはソフトウェアとハードウェアを組み合わせることによって実装されてもよいことに留意されたい。これは、本明細書において限定されない。

30

【0331】

本出願の一実施形態は、スマートコックピット製品を更に提供し、スマートコックピット製品は、前述の第1ノード及び／又は前述の第2ノードを含む。

【0332】

本出願の一実施形態は、インテリジェントデバイス又は輸送車両を更に提供し、車両は、第1ノード及び／又は第2ノードを含む。具体的には、インテリジェントデバイスはロボット等であり得、輸送車両はスマートカー、無人航空機、無人輸送車両等であり得る。

【0333】

実装に関する前述の説明は、簡便かつ簡潔な説明のために、前述の機能モジュールへの分割は単に説明のための例示として使用されることを当業者が明確に理解することを可能にする。実際の適用では、前述の機能を、要求に基づいて実装のために異なる機能モジュールに割り当てることができる、すなわち、装置の内部構造は異なる機能モジュールに分割され、上述の機能の全部又は一部を実装する。

40

【0334】

本出願において提供されるいくつかの実施形態において、開示された装置及び方法は、他の方式で実装されてもよいことを理解されたい。例えば記載される装置の実施形態は単なる例である。例えばモジュール又はユニットへの分割は、単に論理関数分割である。実際の実装においては別の分割方式が存在することがある。例えば複数のユニット又は構成要素が組み合わされるか又は別の装置に組み込まれてよく、あるいはいくつかの特徴が無視されるか又は実行されなくてよい。加えて、表示又は議論された相互結合、直接結合又

50

は通信接続は、いくつかのインタフェースを使用することによって実装され得る。装置又はユニット間の間接的な結合又は通信接続は、電子的、機械的又は別の形態で実装され得る。

【0335】

別個の構成要素として説明されるユニットは、物理的に分離していても、物理的に分離していなくてもよく、ユニットとして表示される構成要素は、1つ以上の物理的ユニットであってよい、すなわち、1つの場所に配置されてよく、あるいは複数の異なる場所に分散されてもよい。ユニットの一部又はすべては、実施形態の解決策の目的を達成するために、実際の要件に基づいて選択されてよい。

【0336】

加えて、本出願の実施形態における機能ユニットは、1つの処理ユニットに統合されてよく、あるいはユニットの各々は、物理的に単独で存在してよく、あるいは2つ以上のユニットが1つのユニットに統合されてもよい。統合ユニットは、ハードウェアの形態で実装されてよく、あるいはソフトウェア機能ユニットの形態で実装されてもよい。

【0337】

統合ユニットがソフトウェア機能ユニットの形態で実装されて、独立した製品として販売又は使用されるとき、統合ユニットは、読取可能記憶媒体に記憶されることがある。このような理解に基づいて、本質的に本出願の実施形態における技術的解決策、先行技術に寄与する部分又は技術的解決策のすべて若しくは一部が、ソフトウェア製品の形態で実装されることがある。ソフトウェア製品は、記憶媒体に記憶され、デバイス（シングルチップマイクロコンピュータ、チップ等であり得る）又はプロセッサ（processor）に、本出願の実施形態で説明される方法のステップのすべて又は一部を実行するよう指示するためのいくつかの命令を含む。前述の記憶媒体は、USBフラッシュドライブ、取外可能ハードディスク、ROM、RAM、磁気ディスク又は光ディスクのような、プログラムコードを記憶することができる任意の媒体を含む。

【0338】

前述の説明は、単に本出願の具体的な実装にすぎないが、本出願の保護範囲を限定するよう意図されていない。本出願で開示される技術的範囲内の変更又は置換は、本出願の保護範囲内にあるものとする。したがって、本出願の保護範囲は、特許請求の範囲の保護範囲に従うものとする。

10

20

30

40

50

【図面】
【図 1】

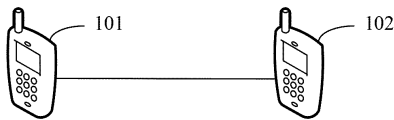


FIG. 1

【図 2】

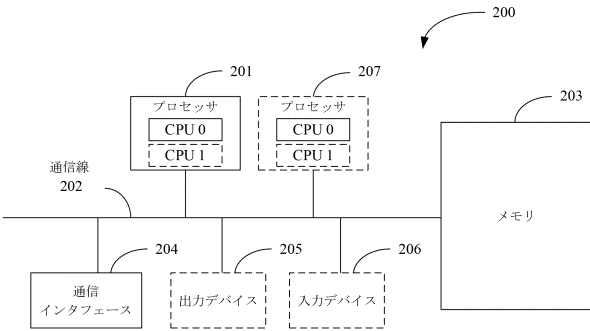


FIG. 2

【図 3】

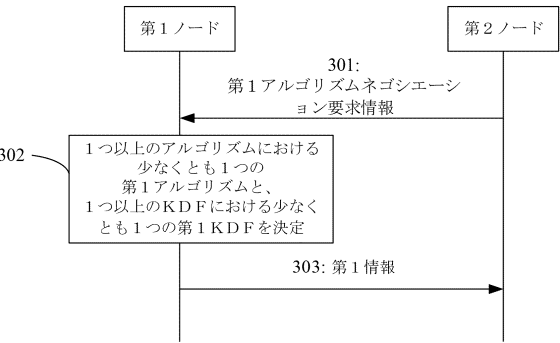


FIG. 3

【図 4】

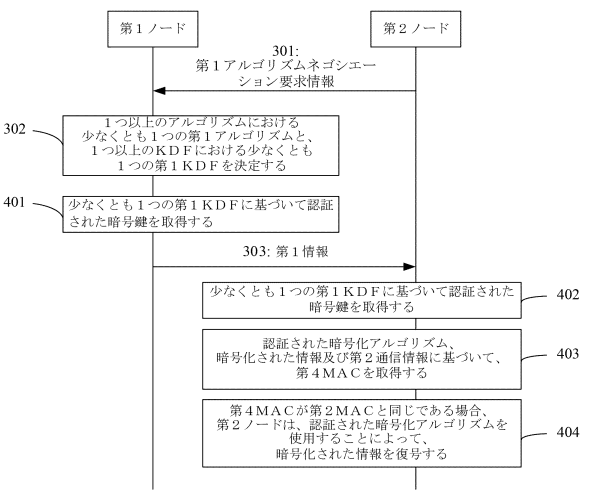


FIG. 4

10

20

30

40

50

【図 5】

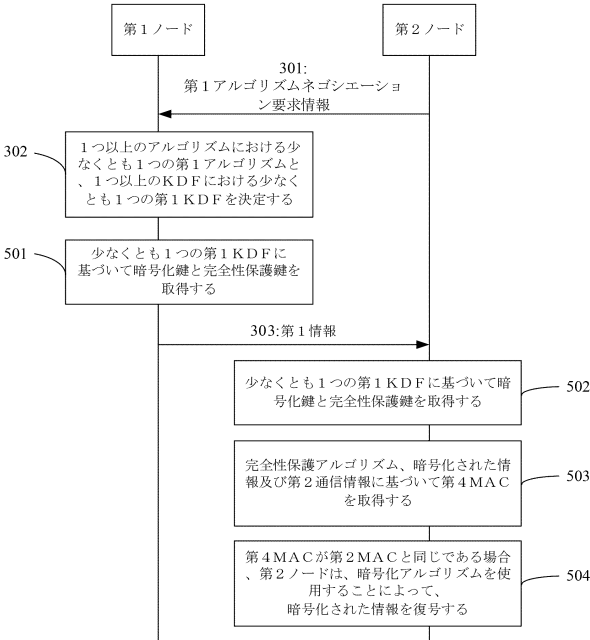


FIG. 5

【図 6】

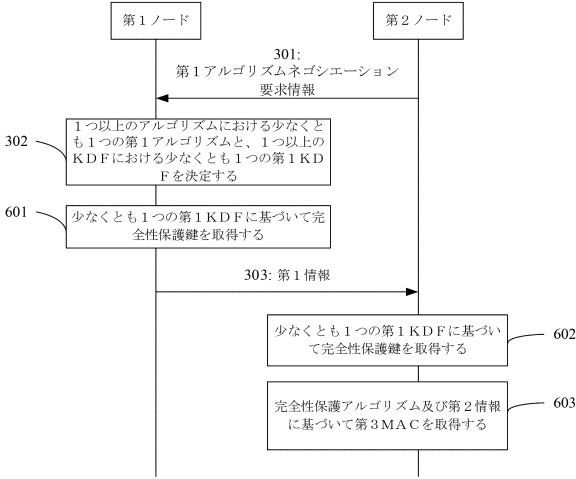


FIG. 6

【図 7】

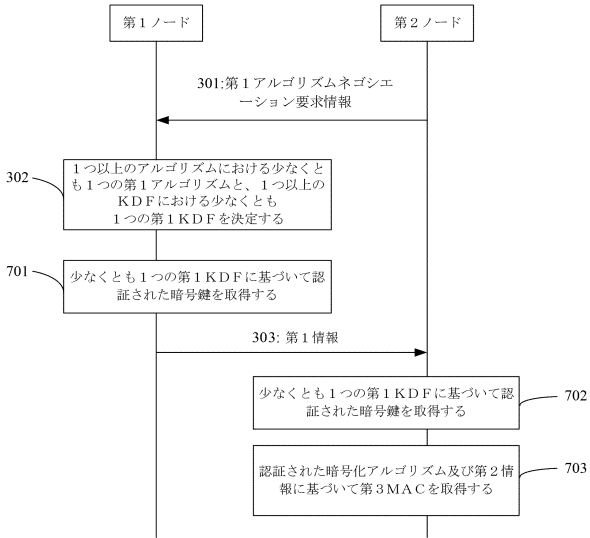


FIG. 7

【図 8】

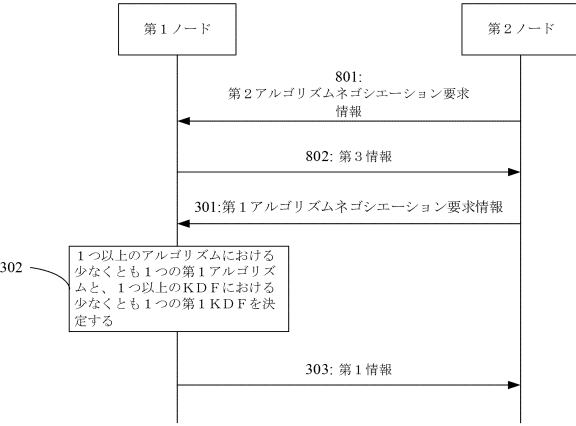


FIG. 8

10

20

30

40

50

【図 9】

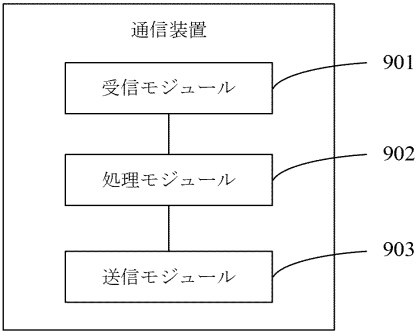


FIG. 9

【図 1 0】

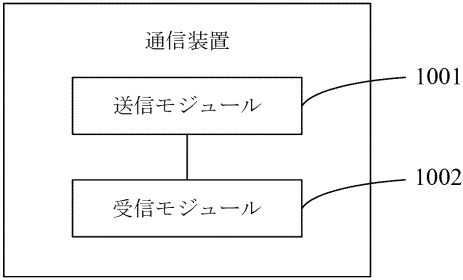


FIG. 10

10

【図 1 1】

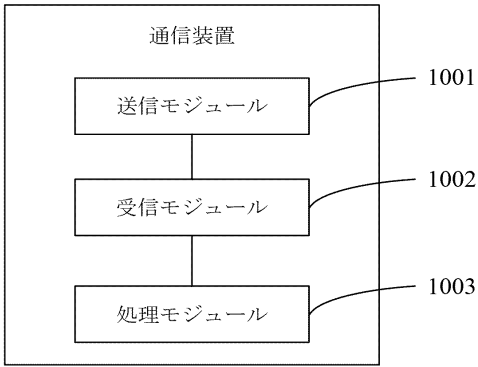


FIG. 11

【図 1 2】

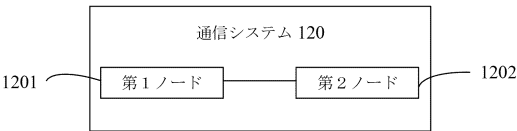


FIG. 12

20

30

40

50

【図 13】

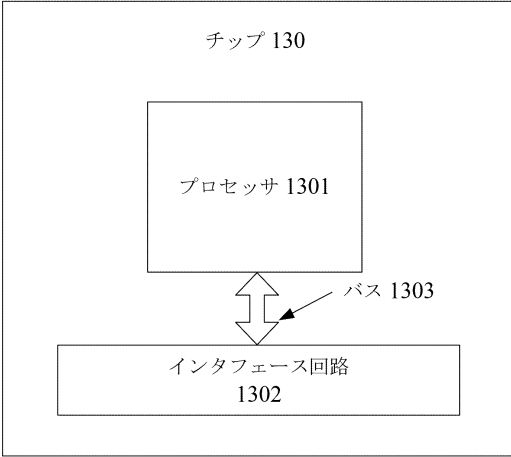


FIG. 13

10

20

30

40

50

フロントページの続き

- (74)代理人 100070150
弁理士 伊東 忠彦
- (74)代理人 100135079
弁理士 宮崎 修
- (72)発明者 ワン, ヨン
中国 5 1 8 1 2 9 グァンドン シェンチェン ロンガン・ディストリクト バンティエン ホアウ
エイ・アドミニストレーション・ビルディング
- (72)発明者 チェン, ジン
中国 5 1 8 1 2 9 グァンドン シェンチェン ロンガン・ディストリクト バンティエン ホアウ
エイ・アドミニストレーション・ビルディング
- 審査官 横田 有光
- (56)参考文献 中国特許出願公開第109905348 (CN, A)
米国特許出願公開第2013/0310006 (US, A1)
中国特許出願公開第106899562 (CN, A)
中国特許出願公開第109560919 (CN, A)
- (58)調査した分野 (Int.Cl., DB名)
H04B 7/24-7/26
H04W 4/00-99/00
3GPP TSG RAN WG1-4
SA WG1-4
CT WG1、4