【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】令和4年10月21日(2022.10.21)

【公開番号】特開2021-64910(P2021-64910A)
【公開日】令和3年4月22日(2021.4.22)
【年通号数】公開・登録公報2021-019
【出願番号】特願2019-189803(P2019-189803)
【国際特許分類】
Ｈ０４Ｗ12/04(2021.01)
Ｈ０４Ｗ84/12(2009.01)
Ｈ０４Ｗ12/06(2021.01)
Ｇ０６Ｆ13/00(2006.01)
Ｈ０４Ｌ　9/08(2006.01)
【ＦＩ】
Ｈ０４Ｗ 12/04
Ｈ０４Ｗ 84/12
Ｈ０４Ｗ 12/06
Ｇ０６Ｆ 13/00 ３５３Ｖ
Ｈ０４Ｌ　9/00 ６０１Ｃ

【手続補正書】
【提出日】令和4年10月13日(2022.10.13)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
通信装置であって、
公開鍵を用いて、他の通信装置とＷｉ－Ｆｉ　Ｄｅｖｉｃｅ　Ｐｒｏｖｉｓｉｏｎｉｎｇ　Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠した認証処理を行う認証手段と、
前記認証手段による前記認証処理に成功した場合であって、前記他の通信装置にＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｏｆ　Ｅｑｕａｌｓ）に対応する通信パラメータを提供する場合に、ＳＡＥのパスワードと、ＰＭＫ（Ｐａｉｒｗｉｓｅ　Ｍａｓｔｅｒ　Ｋｅｙ）の算出に用いられる情報要素とを含む通信パラメータを提供する提供手段と、
を有することを特徴とする通信装置。
【請求項２】
前記通信パラメータに前記情報要素を含ませるかを判定する第１の判定手段を更に有し、
前記提供手段は、前記第１の判定手段によって前記通信パラメータに前記情報要素を含ませると判定された場合に、ＳＡＥの前記パスワードと前記情報要素とを含む前記通信パラメータを提供することを特徴とする請求項１に記載の通信装置。
【請求項３】
前記第１の判定手段は、前記通信パラメータに含まれるＡｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｔｙｐｅ（ＡＫＭ）にＳＡＥが含まれる場合は、前記通信パラメータに前記情報要素を含ませると判定し、前記ＡＫＭにＳＡＥが含まれない場合は、前記通信パラメータに前記情報要素を含ませないと判定することを特徴とす

る請求項２に記載の通信装置。
【請求項４】
前記第１の判定手段は、前記通信装置が前記通信パラメータとして前記情報要素を保持している場合は、前記通信パラメータに前記情報要素を含ませると判定し、前記通信装置が前記通信パラメータとして前記情報要素を保持していない場合は、前記通信パラメータに前記情報要素を含ませないと判定することを特徴とする請求項２に記載の通信装置。
【請求項５】
前記他の通信装置が前記情報要素を利用するかを判定する第２の判定手段を更に有し、
前記第１の判定手段は、前記第２の判定手段によって前記他の通信装置が前記情報要素を利用すると判定された場合は、前記通信パラメータに前記情報要素を含ませると判定し、前記第２の判定手段によって前記他の通信装置が前記情報要素を利用しないと判定された場合は、前記通信パラメータに前記情報要素を含ませないと判定することを特徴とする請求項２に記載の通信装置。
【請求項６】
前記第２の判定手段は、前記他の通信装置から受信した信号に、前記情報要素を利用したＳＡＥに対応していることを示す情報が含まれていた場合は、前記他の通信装置が前記情報要素を利用すると判定し、前記情報要素を利用したＳＡＥに対応していることを示す情報が含まれていなかった場合は、前記他の通信装置が前記情報要素を利用しないと判定することを特徴とする請求項５に記載の通信装置。
【請求項７】
前記第１の判定手段によって、前記通信パラメータに前記情報要素を含ませないと判定された場合、前記通信パラメータには、ＤＰＰのコネクタと、ＰＳＫ（Ｐｒｅ　Ｓｈａｒｅｄ　Ｋｅｙ）と、パスフレーズとの少なくとも何れか一つが含まれることを特徴とする請求項２から６の何れか１項に記載の通信装置。
【請求項８】
前記情報要素は、ＳＡＥのＰａｓｓｗｏｒｄ　Ｉｄｅｎｔｉｆｉｅｒであることを特徴とする請求項１から７の何れか１項に記載の通信装置。
【請求項９】
前記提供手段によって前記情報要素が含まれる前記通信パラメータが提供される場合、前記通信パラメータには、ＳＡＥの前記パスワードと、前記情報要素と、ＳＳＩＤ（Ｓｅｒｖｉｃｅ　Ｓｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）と、ＡＫＭが含まれることを特徴とする請求項１から８の何れか１項に記載の通信装置。
【請求項１０】
前記他の通信装置は、前記提供手段によって提供された前記通信パラメータに含まれる前記パスワードと前記情報要素と楕円曲線暗号とを用いてＰＭＫを算出し、更に前記ＰＭＫを用いて生成したＰＴＫ（Ｐａｉｒ－ｗｉｓｅ　Ｔｒａｎｓｉｅｎｔ　Ｋｅｙ）を用いて通信を行うことを特徴とする請求項１から９の何れか１項に記載の通信装置。
【請求項１１】
前記提供手段は、前記通信パラメータを含むＤＰＰ規格に準拠したＤＰＰ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｒｅｓｐｏｎｓｅを送信することで、前記他の通信装置に前記通信パラメータを提供することを特徴とする請求項１から１０の何れか１項に記載の通信装置。
【請求項１２】
前記提供手段によって提供される前記通信パラメータは、パラメータとして、Ｗｉ－Ｆｉ　Ｔｅｃｈｎｏｌｏｇｙ　Ｏｂｊｅｃｔと、ＳＳＩＤと、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｔｙｐｅとを含み、更に、Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ　Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ　Ｔｙｐｅの値に応じて、Ｐｒｅ－ｓｈａｒｅｄ　ｋｅｙと、ＷＰＡ２　Ｐａｓｓｐｈｒａｓｅと、ＳＡＥ　ｐａｓｓｗｏｒｄと、ＳＡＥ　Ｉｄｅｎｔｉｆｉｅｒと、ＤＰＰ　Ｃｏｎｎｅｃｔｏｒと、Ｃ－ｓｉｇｎ－ｋｅｙと、の少なくとも何れか一つを含むことを特徴とする請求項１から１１の何れか１項に記載の通信装置。

【請求項１３】
通信装置の制御方法であって、
公開鍵を用いて、他の通信装置とＷｉ－Ｆｉ Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠した認証処理を行う認証工程と、
前記認証工程における前記認証処理に成功した場合であって、前記他の通信装置にＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ Ｅｑｕａｌｓ）に対応する通信パラメータを提供する場合に、前記通信パラメータがＳＡＥのパスワードと、ＰＭＫの算出に用いられる情報要素とを含む通信パラメータを提供する提供工程と、
を有することを特徴とする制御方法。
【請求項１４】
請求項１から１２のいずれか１項に記載の通信装置としてコンピュータを動作させるためのプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】
上記目的を達成するため、本発明の通信装置は、公開鍵を用いて、他の通信装置とＷｉ－Ｆｉ Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＰＰ）規格に準拠した認証処理を行う認証手段と、前記認証手段による前記認証処理に成功した場合であって、前記他の通信装置にＳＡＥ（Ｓｉｍｕｌｔａｎｅｏｕｓ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｏｆ Ｅｑｕａｌｓ）に対応する通信パラメータを提供する場合に、ＳＡＥのパスワードと、ＰＭＫ（Ｐａｉｒｗｉｓｅ Ｍａｓｔｅｒ Ｋｅｙ）の算出に用いられる情報要素とを含む通信パラメータを提供する提供手段と、を有する。