【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成29年6月15日(2017.6.15)

【公表番号】特表2016-504874(P2016-504874A)
【公表日】平成28年2月12日(2016.2.12)
【年通号数】公開・登録公報2016-010
【出願番号】特願2015-548660(P2015-548660)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成29年4月25日(2017.4.25)
【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】
ネットワークデバイスの外部で実行される、鍵共有のために当該ネットワークデバイスを構成する方法であって、
各パラメータセットが秘密モジュラス、公開モジュラス、及び整数係数を有する二変数多項式を含む少なくとも２つの当該パラメータセットを、初期化情報として電子形式で取得するステップであって、前記公開モジュラスのバイナリ表現及び前記秘密モジュラスのバイナリ表現は、少なくとも鍵長の連続ビットにおいて同じである、ステップと、
前記初期化情報を用いて前記ネットワークデバイスのローカルキー材料を生成するステップであって、少なくとも
前記ネットワークデバイスの識別番号を電子形式で取得するステップと、
多項式操作デバイスを使用して、前記二変数多項式に前記識別番号を代入し、前記代入の結果にリダクションモジュロ前記パラメータセットの前記秘密モジュラスを行い、前記パラメータセットの前記二変数多項式から一変数多項式を決定することにより、前記初期化情報のパラメータセットごとに対応する一変数多項式を取得するステップとによる、ステップと、
前記各パラメータセットの前記公開モジュラス及び前記各パラメータセットの前記対応する一変数多項式を含む生成された前記ローカルキー材料を前記ネットワークデバイスにおける電子的記憶のために供給するステップと
を含む、方法。
【請求項２】
前記ネットワークデバイスのローカルキー材料を生成する前記ステップは、
前記少なくとも２つのパラメータセットのうちの少なくとも２つに関して、
前記パラメータセットに対応する非ゼロ難読化多項式を生成するステップと、
前記多項式操作デバイスを使用して、前記非ゼロ難読化多項式を前記パラメータセットに対応する前記一変数多項式に加えて難読化された一変数多項式を得るステップとを含み、
前記生成されたローカルキー材料は前記難読化された一変数多項式を含む、請求項１に記載の方法。

【請求項３】
前記難読化多項式の和の各係数は、２の前記鍵長乗の倍数である、請求項２に記載の方法。
【請求項４】
前記難読化多項式の和の各係数を２のべき乗で割り、整数に切り捨てしたものは、２の前記鍵長乗の倍数である、請求項２に記載の方法。
【請求項５】
全てのパラメータセット内の全ての二変数多項式が対称多項式である、請求項１又は２に記載の方法。
【請求項６】
全てのパラメータセットにおいて、各パラメータセットの前記公開モジュラスのバイナリ表現の前記同じ少なくとも鍵長の連続ビットが、各パラメータセットの前記秘密モジュラスの前記鍵長の最下位ビットと同じある、請求項１乃至５のいずれか一項に記載の方法。
【請求項７】
前記少なくとも鍵長の連続ビットは、前記鍵長の最下位ビットである、請求項６に記載の方法。
【請求項８】
電子乱数生成部を用いて前記秘密モジュラスを生成するステップ、又は
前記二変数多項式の１つ以上のランダムな係数を生成することにより、電子乱数生成部を用いて前記二変数多項式を生成するステップ
を含む、請求項１乃至７のいずれか一項に記載の方法。
【請求項９】
１つの又は全ての公開モジュラスが$2^{(a+2)b-1} \leq N$を満たし、ここで、Nは前記公開モジュラスを表し、aは前記二変数多項式の次数を表し、bは前記鍵長を表す、請求項１乃至８のいずれか一項に記載の方法。
【請求項１０】
少なくとも２つのパラメータセットが、前記公開モジュラスのバイナリ表現が全ての秘密モジュラスのバイナリ表現と一致する鍵長の連続位置のセットが存在するよう、複数の秘密モジュラス、及び係数モジュロ秘密モジュラスを有する複数の二変数多項式を含み、
前記一変数多項式を決定する前記ステップは、前記識別番号を前記複数の二変数多項式のそれぞれに代入するステップと、リダクションモジュロ対称二変数多項式に対応する前記複数の秘密モジュラスの秘密モジュラスを行うステップと、前記複数のリダクションの複数の結果を加算するステップとを含む、請求項１乃至９のいずれか一項に記載の方法。
【請求項１１】
前記難読化数は、

$$\epsilon_{i,k}^{A}| < 2^{(a+2-k)b-2}$$

であるように生成され、$\varepsilon_{A,i}$は前記難読化数を表し、iは前記係数に対応する単項式の次数を表し、aは前記二変数多項式の次数を表し、bは前記鍵長を表す、請求項１乃至１０のいずれか一項に記載の方法。
【請求項１２】
第１のネットワークデバイスが共有鍵を決定するための方法であって、前記鍵は暗号鍵であり、
前記第１のネットワークデバイスのローカルキー材料を電子形式で取得するステップであって、前記ローカルキー材料は、少なくとも２つの一変数多項式及び対応する公開モジュラスを含む、ステップと、
前記第１のネットワークデバイスとは異なる第２のネットワークデバイスの識別番号を取得するステップと、

前記少なくとも２つの一変数多項式のそれぞれに関して、前記第２のネットワークデバイスの前記識別番号を前記一変数多項式に代入して、前記代入の結果にリダクションモジュロ前記一変数多項式に対応する前記公開モジュラスを行うステップと、
前記リダクションモジュロ公開モジュラスの結果を足し合わせ、リダクションモジュロ鍵モジュラスを行うステップと、
前記リダクションモジュロ前記鍵モジュラスの結果から前記共有鍵を導出するステップと
を含む、方法。
【請求項１３】
前記第１のネットワークデバイス及び前記第２のネットワークデバイスが同じ共有鍵を導出したか否かを決定し、同じ共有鍵が導出されなかったと決定された場合、前記リダクションモジュロ前記鍵モジュラスの結果から更なる共有鍵を導出するステップを含む、請求項１２に記載の方法。
【請求項１４】
前記代入の結果モジュロ前記公開モジュラスを、２のべき乗である０ビット列除数によって割るステップと、前記除算の結果を整数に切り捨てするステップとを含み、前記０ビット列除数は１より大きい、請求項１２又は１３に記載の方法。
【請求項１５】
共有鍵を決定可能なネットワークデバイスであって、前記鍵は暗号鍵であり、前記ネットワークデバイスは、
前記ネットワークデバイスのローカルキー材料を電子形式で取得するためのローカルキー材料取得部であって、前記ローカルキー材料は少なくとも２つの一変数多項式及び対応する公開モジュラスを含む、ローカルキー材料取得部と、
他のネットワークデバイスの識別番号を取得するための受信部と、
前記少なくとも２つの一変数多項式のそれぞれに関して、前記第２のネットワークデバイスの前記識別番号を前記一変数多項式に代入し、前記代入の結果にリダクションモジュロ前記一変数多項式に対応する前記公開モジュラスを行い、前記リダクションモジュロ公開モジュラスの結果を足し合わせてリダクションモジュロ鍵モジュラスを行うための多項式操作デバイスと、
前記リダクションモジュロ前記鍵モジュラスの結果から前記共有鍵を導出するための鍵導出デバイスと
を含む、ネットワークデバイス。
【請求項１６】
鍵共有のためにネットワークデバイスを構成するためのシステムであって、
秘密モジュラス、公開モジュラス、及び整数係数を有する二変数多項式を含む少なくとも２つのパラメータセットを、電子形式で取得するための鍵材料取得部であって、前記公開モジュラスのバイナリ表現及び前記秘密モジュラスのバイナリ表現は、少なくとも鍵長の連続ビットにおいて同じである、鍵材料取得部と、
前記ネットワークデバイスのローカルキー材料を生成するための生成部であって、
前記ネットワークデバイスの識別番号を電子形式で取得するための、及び、生成された前記ローカルキー材料を前記ネットワークデバイスに電子的に保存するためのネットワークデバイスマネージャーと、
前記二変数多項式に前記識別番号を代入し、前記代入の結果にリダクションモジュロ前記パラメータセットの前記秘密モジュラスを行い、前記パラメータセットの前記二変数多項式から一変数多項式を決定することにより、パラメータセットごとに対応する一変数多項式を取得するための多項式操作デバイスとを含む、生成部と
を含むシステム。
【請求項１７】
鍵共有のためにネットワークデバイスを構成する方法を、前記ネットワークデバイスの外部のプロセッサに実行させるための命令を含むプログラムを含む、非一時的コンピュー

タ可読記憶媒体であって、前記方法は、
各パラメータセットが秘密モジュラス、公開モジュラス、及び整数係数を有する二変数多項式を含む少なくとも２つの当該パラメータセットを、初期化情報として電子形式で取得するステップであって、前記公開モジュラスのバイナリ表現及び前記秘密モジュラスのバイナリ表現は、少なくとも鍵長の連続ビットにおいて同じである、ステップと、
初期化情報として前記ネットワークデバイスのローカルキー材料を生成するステップであって、
前記ネットワークデバイスの識別番号を電子形式で取得するステップと、
多項式操作デバイスを使用して、前記二変数多項式に前記識別番号を代入し、前記代入の結果にリダクションモジュロ前記パラメータセットの前記秘密モジュラスを行い、前記パラメータセットの前記二変数多項式から一変数多項式を決定することにより、前記初期化情報のパラメータセットごとに対応する一変数多項式を取得するステップとを含む、ステップと、
前記各パラメータセットの前記公開モジュラス及び前記各パラメータセットの前記対応する一変数多項式を含む生成された前記ローカルキー材料を前記ネットワークデバイスにおける電子的記憶のために供給するステップと
を含む、非一時的コンピュータ可読記憶媒体。