(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6190470号
(P6190470)
(45)発行日　平成29年8月30日(2017.8.30)　(24)登録日　平成29年8月10日(2017.8.10)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E

請求項の数 17　(全 33 頁)

(21)出願番号　特願2015-548660(P2015-548660)
(86)(22)出願日　平成25年12月20日(2013.12.20)
(65)公表番号　特表2016-504874(P2016-504874A)
(43)公表日　平成28年2月12日(2016.2.12)
(86)国際出願番号　PCT/EP2013/077842
(87)国際公開番号　WO2014/096420
(87)国際公開日　平成26年6月26日(2014.6.26)
審査請求日　平成28年12月19日(2016.12.19)
(31)優先権主張番号　12198794.5
(32)優先日　平成24年12月21日(2012.12.21)
(33)優先権主張国　欧州特許庁(EP)
(31)優先権主張番号　61/740,488
(32)優先日　平成24年12月21日(2012.12.21)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
KONINKLIJKE PHILIPS N.V.
オランダ国　5656　アーエー　アインドーフェン　ハイテック　キャンパス　5
High Tech Campus 5, NL-5656 AE Eindhoven
(74)代理人　110001690
特許業務法人M&Sパートナーズ

最終頁に続く

(54)【発明の名称】鍵共有ネットワークデバイス及びその構成

(57)【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。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、鍵共有のためにネットワークデバイスを構成する方法に関連し、方法は、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を含み、当該生成するステップは、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、二変数多項式に識別番号を代入することにより、多項式操作デバイスを用いて二変数多項式から一変数多項式を決定するステップと、生成されたローカルキー材料をネットワークデバイスに電子的に保存するステップとを含む。
【０００２】
本発明は、更に、第１のネットワークが共有鍵を決定するための方法に関連し、鍵は暗号鍵であり、方法は、一変数多項式を含む第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と、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、第２のネットワークデバイスの識別番号を一変数多項式に代入し、それから共有鍵を導出するステップとを含む。
【０００３】
本発明は、更に、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、及び、共有鍵を決定するよう構成されたネットワークデバイスに関する。
【背景技術】
【０００４】
SONG GUOらによる論文"A Permutation-Based Multi-Polynomial Scheme for Pairwise Key Establishment in Sensor Networks", COMMUNICATIONS (ICC), 2010 IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 23 May 2010 (2010-05-23), pp.1-5は、従来技術のソリューションを開示する。

【０００５】
複数のネットワークデバイスを含む通信ネットワークにおいて、かかるネットワークデバイスのペア間に安全な接続を確立することは課題である。これを達成する方法の１つが、C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M Yung, “Perfectly-Secure Key distribution for Dynamic Conferences”, Springer Lecture Notes in Mathematics, Vol. 740, pp. 471-486, 1993(「Blundo」と呼ぶ）に開示されている。
【０００６】
この方法は、p個の元を含む有限体F内の係数を有する対称二変数多項式f(x,y)（pは素数又は素数のべき乗）を生成する中央権限（ネットワーク権限又は信頼できる第３者機関（Trusted Third Party; TTP）とも呼ばれる）を仮定する。各デバイスはF内に識別番号を有し、TTPからローカルキー材料を受け取る。識別子ηのデバイスのローカルキー材料は、多項式f(η, y)の係数である。
【０００７】
デバイスηがデバイスη’と通信したい場合、デバイスηは鍵材料を用いて鍵K(η, η’)=f(η, η’)を生成する。fは対称式なので、同じ鍵が生成される。
【０００８】
攻撃者がt+1以上のデバイスの鍵材料を知る場合、この鍵共有スキームには問題が生じる（tは二変数多項式の次数）。この場合、攻撃者は多項式f(x,y)を復元することができ、システムのセキュリティはその瞬間に完全に崩壊する。任意の２つのデバイスの識別番号が与えられれば、攻撃者はそのデバイスペア間で共有される鍵を復元することができる。
【発明の概要】
【発明が解決しようとする課題】
【０００９】
２つのネットワークデバイス間で共有鍵を確立するための改良された方法を得ることは有益であろう。本発明は独立請求項によって定められ、従属請求項は好適な実施形態を定める。鍵共有のためにネットワークデバイスを構成する方法、及びネットワークデバイスが共有鍵を決定するための方法が提供される。
【課題を解決するための手段】
【００１０】
鍵共有のためにネットワークデバイスを構成する方法は、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ステップであって、公開モジュラスのバイナリ表現及び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、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、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、二変数多項式に識別番号を代入し、代入の結果にリダクションモジュロパラメータセットの秘密モジュラスを行い、パラメータセットの二変数多項式から一変数多項式を決定することにより、少なくとも２つのパラメータセットのそれぞれに関して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、各パラメータセットの公開モジュラス及び各パラメータセットの対応する一変数多項式を含む生成されたローカルキー材料をネットワークデバイスに電子的に保存するステップとを含む。
【００１１】
第１のネットワークデバイスが暗号鍵である共有鍵を決定するための方法は、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、ローカルキー材料は、少なくとも２つの、オプションで難読化され得る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、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、少なくとも２つのオプションで難読化され得る一変数多項式のそれぞれに関して、第２のネットワークデバイスの識別番号

を一変数多項式に代入して、代入の結果にリダクションモジュロ一変数多項式に対応する公開モジュラスを行うステップと、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、リダクションモジュロ鍵モジュラスの結果から共有鍵を導出するステップとを含む。

【００１２】

一実施形態では、方法は、代入の結果にリダクションモジュロ公開モジュラスを行うステップと、その結果を２のべき乗で割るステップと、リダクションモジュロ鍵モジュラスを行うステップとを含む。

【００１３】

それぞれが識別番号及びその識別番号のために生成されたローカルキー材料を有する複数のネットワークデバイス中の任意の２つのネットワークデバイスのペアは、共有鍵について少しの資源で協議することができる。２つのネットワークデバイスは、秘密にされる必要がない識別番号を交換して多項式計算を行うだけでよい。必要とされる計算の種類は大きな計算資源を要求せず、これはこの方法が低コスト且つハイボリュームな種類のアプリケーションに適していることを意味する。

【００１４】

ローカルキー材料はルートキー材料内の共通の多項式から取得される。これは、ネットワークデバイスペアの両ネットワークデバイスが同じ共有鍵を取得することを可能にする。全ての二変数多項式が対称の場合、任意の２つのネットワークデバイスが共通の多項式を導出し得る。一部の又は全ての二変数多項式が非対称の場合、一部のデバイスペアは共有鍵を導出することができ、一部のペアは導出することができない。

【００１５】

ローカルキー材料はパラメータセットから、特に複数の異なる公開モジュラス及び複数の二変数多項式から導出される。結果のローカルキー材料は、それぞれが対応する公開モジュラスを有する、複数の典型的には異なる一変数多項式を含む。

【００１６】

１つのパラメータセットしか使用されない場合、ネットワークデバイスには多項式の係数が提供され、モジュロＮを評価してbビットを取ることにより、任意の他のデバイスとbビットの鍵を生成することができる。これは、いわゆるノイジー多項式補間問題に関連し、すなわち、これらのbビット鍵を多数有することにより、攻撃者は攻撃対象の所与の機関の多項式を復元可能であり得る。

【００１７】

例えば、単一のパラメータセットシステムに対する攻撃は、次の２つのステップによりこれらのｂビット値を取得し得る。攻撃者はN_cの鍵材料に関連付けられたN_cのデバイスを危殆化し、これらのN_cの鍵材料を使用してN_cのｂビット鍵を取得する（攻撃対象のデバイスの識別子において各鍵材料を評価することにより）。これは、ノイジー多項式補間問題に関する進歩が、単一のパラメータセットシステムに対する攻撃に拡張し得ることを意味する。これは望ましくないと考えられる。

【００１８】

複数のパラメータセットを有することは、デバイス上で及びローカルキー生成中にモジュロ演算を混合することにより、この問題を防ぐ。

【００１９】

デバイスA及びBのペア間で共有される共通鍵K_{AB}は、少なくとも２つの（一般的にはｍ̀の）サブキー

$$K_{AB}^{i}$$

の和として得られ、すなわち

$$K_{AB} = K_{AB}^{1} + K_{AB}^{2}$$

である。各サブキー

K_{AB}^{i}

は、モジュロ公開モジュラスNのモジュロ演算が実行される異なる鍵材料から生成される。ローカルキー生成中及び共有鍵生成中にモジュロ演算が混合されるため、ノイジー多項式補間攻撃を暗号システムに拡張することはできない。たとえ攻撃者がN_cのbビット鍵を入手可能であったとしても、それぞれが２つのサブキーから導出され、各サブキーは異なる鍵材料の評価に由来する。しかし、攻撃者はサブキーを区別することができないので、攻撃者は攻撃対象のデバイスの２つの（一般的にはm の）鍵材料を復元することができない。

【００２０】

デバイスに対する攻撃には２つのレベルの深刻度が存在する。低い方の深刻度では、攻撃者は多数の共通の共有鍵へのアクセスを有するだけである。高い方の深刻度では、攻撃者は多数のローカルキー材料へのアクセスを有する。ネットワークデバイスにおける混合モジュロ演算を有することは、低い方の深刻度の攻撃に対する良好な対策である。しかし、攻撃者が鍵材料自体へのアクセスを有する場合、攻撃者はサブキーへのアクセスも有する。

【００２１】

後者の問題は、デバイスの２つの鍵材料にノイズを加えることによって防がれる。ローカルキー材料に難読化数を加えると、ローカルキー材料とルートキー材料との間の関係は乱される。難読化されていない一変数多項式と（対称）二変数多項式との間に存在していた関係は無くなる。これは、かかるスキームに対する単純な攻撃が通用しなくなることを意味する。

【００２２】

興味深いことに、ノイズの和が0モジュロ2^bになるようデバイスの２つの鍵材料にノイズを加えることにより、システムは更に改良される。この場合、生成された鍵は依然としてノイジーであり、よって、攻撃者はそれらを使用して攻撃対象のデバイスの鍵材料シェアを復元することはできない。しかし、ノイズを除去するには、攻撃者はそれらを加算しなければならないが、その場合は上記のように和が得られ、各鍵材料に由来する成分を区別することができない。この技術は任意の数の鍵材料に容易に一般化することができる。ノイズがLSBではなく他の箇所に位置するbビットにおいてゼロになることを保証するよう条件を拡張してもよい。

【００２３】

一実施形態では、各パラメータセット内の全ての公開モジュラスのバイナリ表現及び秘密モジュラスのバイナリ表現は、少なくとも鍵長（b）の連続ビットにおいて同じである。複数の秘密モジュラスが使用されてもよいことに留意されたい。複数の秘密モジュラスは、公開モジュラスの複数の秘密モジュラスの任意の１つのバイナリ表現及び秘密モジュラスのバイナリ表現が少なくとも鍵長（b）の連続ビットにおいて同じであるよう選択され得る。複数の秘密モジュラスの秘密モジュラスごとに、整数の係数を有し、対称であり得る二変数多項式が選択され、複数の任意で対称な二変数関数が得られる。

【００２４】

ローカルキー材料の導出は公開モジュラスとは異なる秘密モジュラスを使用するため、例えば単一の有限体内で作業する場合に存在するであろう数学的関係は妨害される。これは、多項式解析のための通常の数学的ツール、例えば有限代数が適用できなくなることを意味する。攻撃者はせいぜい格子等のはるかに非効率的な構造を使用し得る。また、共有鍵を導出する際、通常の数学的意味では両立しない（not compatible）２つのモジュロ演算が組み合わされる。したがって、数学的構造は２箇所で回避される。方法は直接的なペアワイズ鍵生成を可能にし、非常に多くの、例えば10^5オーダーの、場合によってはそれ以上のネットワークデバイスを取り込むレジリエンスを有する。一方、秘密モジュラス

及び公開モジュラスは複数の連続ビットにおいて重複するため、ローカルキー材料を有する２つのネットワークデバイスが同じ共有鍵を導出できる可能性は高い。

【００２５】

発明者の特定の一洞察は、公開モジュールが素数でなくともよいということであった。一実施形態では、公開モジュラスは合成数である。また、公開モジュラスがバイナリ表現で「全て１」ビットの数字、例えば、１ビットのみからなる数字であるべき理由はない。一実施形態では、公開モジュラスは２のべき乗マイナス１ではない。一実施形態では、公開モジュラスのバイナリ表現は少なくとも１つの０ビットを含む（先頭のゼロはカウントしない、すなわち、公開モジュラスは公開モジュラスのMSBより下位の０ビットを少なくとも１つ含む）。一実施形態では、公開モジュラスは２のべき乗マイナス１であり、合成数である。

【００２６】

一実施形態では、１つ以上のパラメータセットの公開モジュラスは１つ以上の秘密モジュラスより大きい。

【００２７】

一実施形態では、公開モジュラスマイナス秘密モジュラスのバイナリ表現の少なくとも鍵長の連続ビットは全て０ビットである。この差は、２の補数表現ではなく、公開モジュラスマイナス秘密モジュラスの符号付数値表現を用いて評価されるべきである。あるいは、公開モジュラスマイナス秘密モジュラスの絶対値のバイナリ表現の少なくとも鍵長の連続ビットが全て０ビットであることが要求され得る。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合致する鍵長（ｂ）の連続位置のセットが存在する。

【００２８】

公開モジュラスが秘密モジュラスと合致する連続ビット位置は、LSB（least significant bits）であり得る。一実施形態では、公開モジュラスマイナス秘密モジュラスのバイナリ表現の最下位の鍵長ビットが全て０ビットである。これは、共有鍵を導出するとき２のべき乗による除算が必要ないという利点を有する。

【００２９】

一実施形態では、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公開モジュラスのバイナリ表現の同じ少なくとも鍵長（ｂ）の連続ビットは、各パラメータセットの秘密モジュラスの鍵長（ｂ）LSBと同じである。すなわち、各パラメータセットにおいて、公開モジュラス及び秘密モジュラスが一致する連続ビット位置のセットが存在する。この連続ビット位置のセットは全てのパラメータセットに関して同じであるが、ビット自体は異なるパラメータセットにわたり異なってもよい。一実施形態では、少なくとも鍵長（ｂ）の連続ビットは、鍵長（ｂ）LSBである。すなわち、ビット位置のセットはLSB位置である。

【００３０】

複数の秘密モジュラス中の１つの秘密モジュラスが公開モジュラスと等しくてもよい。しかし、単一の秘密モジュラスが使用される場合、これは望ましくない。

【００３１】

秘密モジュラスが十分な非線形性を導入することが望ましい。一実施形態では、公開モジュラスが各秘密モジュラスと異なる連続ビット位置のセットが存在する。更に、秘密モジュラス同士が異なることを課されてもよい。秘密モジュラスのバイナリ表現のペアワイズ比較が、例えば少なくとも鍵長の連続ビットのセット内の少なくとも１つのビットにおいて異なってもよく、セットは全ての秘密モジュラスについて等しく、場合によっては公開モジュラスについても同じである。

【００３２】

ネットワークデバイスは、電子通信手段及び計算手段を備える電子デバイスであり得る。ネットワークデバイスは、例えばRFIDタグ形式で任意の非電子物体に取り付けられ得る。例えば、当該方法は「モノのインターネット」に適し得る。例えば、物体、特に低コス

トの物体が、物体が通信するための、例えば識別されるための無線タグを備えてもよい。かかる物体は、コンピュータ等の電子手段を介してインベントリに入れられてもよい。盗難された又は故障したアイテムを容易に追跡及び発見することができる。特に有望な1 つのアプリケーションは、共有鍵を決定するよう構成されたネットワークデバイスを備える照明である。かかる照明は安全に自身の状態を通信し、かかる照明は安全に制御、例えばON／OFFされ得る。ネットワークデバイスは、それぞれが識別番号を送受信するための及び電子ステータスメッセージを送信するための電子通信機を含み、また、それぞれが本発明に係る方法に従い共有鍵を導出するよう構成された集積回路を含む複数のネットワークデバイスの1 つであり得る。

【００３３】

一実施形態では、本発明の方法はIPSec、(D) TLS、HIP、又はZigBee等のセキュリティプロトコルのための暗号化方法として使用され得る。特に、これらのプロトコルのうちの1 つを使用するデバイスは識別子に関連付けられる。第1 のデバイスと通信しようとしている第2 のデバイスは、その識別子に基づき、第1 のデバイスと共通のペアワイズ鍵を生成でき、このペアワイズ鍵(又は例えば鍵導出関数によってこれから導出された鍵) は、事前共有鍵に基づく上記プロトコルの一方法に使用され得る。特に、本発明において規定されるデバイスの識別子は、ZigBeeショートアドレス、IPアドレス、又はホストID等のネットワークアドレスであり得る。また、識別子はデバイスのIEEEアドレスでもよいし、又はデバイスが製造中にIEEEアドレスに関連付けられたローカルキー材料を受信するようデバイスに関連付けられた適切なビット列でもよい。

【００３４】

共有鍵の導出は多数のアプリケーションに使用され得る。典型的には、共有鍵は暗号対称鍵である。対称鍵は機密性のために使用されてもよく、例えば、送信メッセージ又は受信メッセージが対称鍵によって暗号化されてもよい。両方の識別番号、及び2 つのローカルキー材料のうちの1 つを利用できる(又はルートキー材料を利用できる) デバイスのみが通信を解読できる。対称鍵は認証のために使用されてもよく、例えば、送信又は受信メッセージが対称鍵を用いて認証されてもよい。このようにすることで、メッセージの発信源を確認できる。両方の識別番号、及び2 つのローカルキー材料のうちの1 つを利用できる(又はルートキー材料を利用できる) デバイスのみが認証メッセージを作成できる。

【００３５】

鍵共有のためにネットワークデバイスを構成する方法は、典型的にはネットワーク権限、例えばTTPによって実行される。ネットワーク権限は必要な材料、例えばルートキー材料を他のソースから取得してもよいが、自身でこれを生成してもよい。例えば、公開モジュラスが生成され得る。例えば、公開モジュラスがシステムパラメータであって受信されたとしても、秘密モジュラスは生成され得る。

【００３６】

一実施形態では、1 つ以上の又は全ての公開モジュラスNが$2^{(a+2)b-1} \leq N < 2^{(a+2)b}-1$を満たすよう選択され、ここで、aは二変数多項式の次数を表し、bは鍵長を表す。例えば、一実施形態では$N = 2^{(a+2)b}-1$である。後者の選択の場合のモジュロ演算は特に効率的に実行され得る。

【００３７】

固定の公開モジュラスを有することは、それがネットワークデバイスに伝送される必要がなく、例えばネットワークデバイスのシステムソフトウェアに組み込まれ得るという利点を有する。特に、公開モジュラスは乱数生成部を使用して選択されてもよい。

【００３８】

公開モジュラス及び秘密モジュラスはビット列で表現され得る。また、特定の数学的構造を用いてこれらを簡略化してもよい。例えば、秘密モジュラスを記憶する代わりに、はるかに短いであろう公開モジュラスとの差を記憶してもよい。

【００３９】

公開モジュラスマイナス秘密モジュラスのバイナリ表現の「鍵長」数のLSBが全て0 ビ

ットになるように秘密モジュラスを選択することは、ネットワークデバイスペアの第1のネットワークデバイスにおける共有鍵がネットワークデバイスペアの第2のネットワークデバイスにおいて導出される共有鍵に近くなる可能性を高める。すなわち、秘密モジュラスのバイナリ表現は、「鍵長」の最下位の位置において、公開モジュラスのバイナリ表現と同じビットを有する。例えば、鍵長が64の場合、公開モジュラスから2^{64}の倍数を引くことによって秘密モジュラスが選択され得る。一実施形態では、公開モジュラスマイナス秘密モジュラス割る2の鍵長乗は、2の鍵長乗より小さい。

【００４０】

一実施形態では、複数の秘密モジュラスが電子形式で取得又は生成され、複数の秘密モジュラスの秘密モジュラスごとに整数の係数を有する対称二変数多項式が選択されることによって複数の対称二変数多項式が得られ、秘密モジュラスごとに対称二変数多項式が対応する。一変数多項式を決定するステップは、識別番号を複数の対称二変数多項式のそれぞれに代入するステップと、それぞれの対称二変数多項式に複数の秘密モジュラスの対応する秘密モジュラスを法としたリダクションモジュロを行うステップと、複数のリダクションの複数の結果を足し合わせるステップとを含む。異なるモジュラスに対して複数の対称二変数多項式を有する場合、両立しない構造が更に混ぜられるので、セキュリティが高まる。典型的には、秘密モジュラスは互いに異なる。対応する代数的構造が大きく異なる場合、例えば、複数の秘密モジュラスを互いに素になるように、特にペアワイズに互いに素になるように選択することによって、更に特に異なる素数であるように選択することにより、複数の秘密モジュラスを有することは解析を一層複雑にする。

【００４１】

異なる秘密モジュラス、特に複数の秘密モジュラスを有することは、攻撃者による解析を複雑にする。セキュリティを更に高めるために、係数を更に制御してもよい。一実施形態では、複数のリダクションの結果の複数の一変数多項式を足し合わせる権限が、得られた係数の各値が小さ過ぎるか又は大き過ぎるか、例えば、下限閾値未満であるか又は上限閾値以上であるかを検証する。いずれの場合でも、複数のリダクションの要素が大き過ぎる又は小さ過ぎる場合、攻撃者が突き止め得るので、これはセキュリティを更に高める。例えば、加算後の係数の値が1であり、2つの一変数多項式しか存在しない場合、攻撃者は、第1の多項式に関連付けられた対応する係数が1であり、第2の多項式に関連付けられた係数が0であるか、又はその反対であることを知る。特に、デバイスのローカルキー材料を生成する権限が、デバイスのローカルキー材料の得られた係数の各値が「最小値」以上且つ「最大値」以下であるか否かを検証できる。この確認は省略されてもよく、特に、公開モジュラスが全ての秘密モジュラスに比較的近く、鍵材料の全ての要素が0とN-1との間の場合、省略されてもよい。TTPが識別番号を割り当てることができる場合は、TTPが小さい又は大きい係数を発見するとき、TTPはデバイスに別の識別番号を割り当ててもよい。

【００４２】

一実施形態では、特定の秘密モジュラスは、それぞれ、公開モジュラスマイナス特定の秘密モジュラスのバイナリ表現の最下位の鍵長(b)ビットが全て0ビットであるようなものである。

【００４３】

公開モジュラスは秘密モジュラスより大きくても小さくてもよい。一実施形態では、公開モジュラスマイナス秘密モジュラスのバイナリ表現は少なくとも鍵長の全0ビットを有する。少なくとも鍵長の0ビットは連続しており、バイナリ表現内の任意の位置に存在し得る。公開モジュラスと秘密モジュラスとの差に0ビット列を有することは、難読化の度が過ぎることを回避する。ストリングは全てのパラメータセットにわたり存在してもよいが、そうでなくてもよいことに留意されたい。

【００４４】

一実施形態では、公開モジュラスマイナス秘密モジュラスの鍵長のLSB割る2のs乗が全て0になるような整数パラメータ「s」が存在する。パラメータ「s」は全ての秘密モジュ

ラスについて同じであるが、パラメータセットごとに異なってもよい。

【００４５】

例えば、特定の秘密モジュラスそれぞれに関して、公開モジュラスマイナス特定の秘密モジュラス割る０ビット列除数のバイナリ表現の鍵長（ｂ）ビットが全て０ビットであるような０ビット列除数（２のべき乗）が定められてもよい。LSBが０の場合、０ビット列除数は１でもよい。一実施形態では、０ビット列除数は１より大きい。２のべき乗による除算は、LSB方向のビットのシフトと同じ結果を与える整数除算として解釈することができる。除算の剰余は無視される。

【００４６】

鍵長ビットの共有鍵を生成するために、ネットワークデバイスは先に追加の除算ステップを適用する。第１のネットワークデバイスは、パラメータセットごとに、公開モジュラスを法とした第２のデバイスの識別番号の鍵材料モジュロを評価し、結果を加算し、２のs乗で割り、リダクションモジュロ２の鍵長乗を行う。これは、公開モジュロの後にまずモジュロ2のs+鍵長乗を適用し、その後２のs乗で除算することに等しいことに留意されたい。ここで、「除算は」端数の切り捨てを含む。

【００４７】

一実施形態では、秘密モジュラスは乱数生成部を使用して生成される。一実施形態では、複数の秘密モジュラスはペアワイズに互いに素になるように生成される。例えば、新たな秘密モジュラスごとにそれらが依然としてペアワイズに互いに素であることを確認し、そうでない場合、最後に生成された秘密モジュラスを破棄することを繰り返して複数の秘密モジュラスを生成してもよい。一実施形態は、候補モジュラスが素数判定デバイスによる素数判定を満たすまで、乱数生成部を使用して、公開モジュラスマイナス候補モジュラスのバイナリ表現の鍵長（ｂ）の連続ビットが全て０であるような候補モジュラスを繰り返し生成するステップを含み、このようにして得られた素数判定を満たす候補モジュラスが秘密モジュラスとして使用される。素数判定法は、例えばMiller-Rabin素数判定法又はSolovay-Strassen 素数判定法でもよい。

【００４８】

次数aの変数x及びyの対称二変数多項式は、形式$x^i y^j$の単項式しか有さない（$i \leq a$、$j \leq a$）。更に、$x^i y^j$に対応する係数は、$x^j y^i$に対応する係数と同じである。これは、記憶される係数の数を約半分に減らすために利用され得る。より緩和された次数の定義を用いることも可能であることに留意されたい。単項式内の変数の最大次数を単項式の次数として定める。したがって、$x^j y^i$の次数は$\max(i,j)$である（$i \leq a$、$j \leq a$）。したがって、例として、次数１の多項式と呼ばれる式は$a+bx+cy+dxy$のような一般形を有する（対称多項式のみを考慮するので、b= cであることに留意されたい）。望ましい場合、例えば、$i+j \leq a$である単項式のみが使用されるという制約を含め、二変数多項式に追加の制約を課してもよいが、必須ではない。

【００４９】

一実施形態では、対称二変数多項式はネットワーク権限によって生成される。例えば、対称二変数多項式はランダムな対称二変数多項式であり得る。例えば、乱数生成部を使用して係数を乱数として選択してもよい。

【００５０】

使用される難読化は攻撃に対するレジリエンス、特に複数の鍵材料が組み合わせられる結託攻撃に対するレジリエンスを大きく高めるが、潜在的な欠点を有する。場合によっては、第１のネットワークデバイスによって導出された共有鍵は、第２のネットワークデバイスによって導出された共有鍵と全てのビットにおいて同一ではない。これは、難読化係数の加算後のキャリービットにおけるミスマッチに主に起因する。他の原因は、生成されるキャリービットに影響を与える鍵の生成中の各秘密モジュラスのモジュラ効果の欠如である。厄介ではあるが、この欠点は多様な方法で解決できる。難読化をより注意深く選択することにより、差異の可能性、特に大きな差異の可能性を大幅に低減することができる。更に、存在する場合、差異は生成された鍵のLSB内に位置する可能性が高いことがわか

った。したがって、１つ以上のLSBを除去することによって同一の共有鍵の可能性を高めることができる。例えば、共有鍵を決定する方法の一実施形態は、第１のネットワークデバイス及び第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するステップと、同じ鍵が導出されなかったと決定される場合、鍵モジュラスを法としたリダクションモジュロの結果から更なる共有鍵を導出するステップとを含む。両側で等しい鍵が発見されるまで、更なる共有鍵が導出されてもよい。共有鍵に閾値未満のビット数しか残っていない場合、方法は終了する。一部のアプリケーションでは、単純に、ネットワークデバイスのいくらかの割合は通信できないと受け止められ得る。例えば、メッセージが様々なルートを取り得るアドホック無線ネットワークでは、ネットワークデバイスの一部が通信できない場合にも接続性を失うことはない。

【００５１】

一実施形態では、共有鍵の複数のLSBが除去され、除去されるビット数は、例えば1、2以上、4以上、8以上、16以上、32以上、又は64以上であり得る。より多くのLSBを除去することにより、異なる鍵を有する可能性は低くなり、特に、任意の所望の閾値まで下げられ得る。共有鍵が等しくなる可能性は数学的関係に基づいて計算されてもよいし、実験により決定されてもよい。

【００５２】

また、難読化数の選択も制御され、一実施形態では、高次の単項式に対応する係数については、選択される難読化数が選択される範囲が縮小される。特に、$|\varepsilon_{A,i}|<2^{(a+1-i)b}$が要求され、ここで$\varepsilon_{A,i}$はi次の単項式の難読化数を表し、iは係数に対応する単項式の次数を表し、aは二変数多項式の次数を表し、bは鍵長を表す。Aはローカルキー材料が生成される対象のネットワークデバイスを表す。一実施形態では、例えば上記式を用いて、係数ごとに難読化数が生成される。ネットワークデバイスごとに異なる難読化が適用され得る。例えば、３以上のネットワークデバイスが存在する場合であっても、ネットワークデバイスごとに異なる難読化数が生成され得る。

【００５３】

難読化数は正数に制限されてもよいが、これは必須ではなく、難読化数は負でもよいことに留意されたい。一実施形態では、難読化数は乱数生成部を用いて生成される。複数の難読化数を生成し、一変数多項式の係数に加え、難読化された一変数多項式を得てもよい。一変数多項式の１つ以上の、好ましくは全ての係数がこのように難読化され得る。

【００５４】

ネットワークデバイスの識別番号のビット数は、通常、鍵長以下であるよう選択される。識別番号は、例えば32又は64以上のビット列であり得る。鍵長は32以上、48以上、64以上、96以上、128以上、又は256以上でもよい。対応する決定共有鍵のLSBの数を減らすために、鍵長のビット数はいくらか高く選択されてもよい。一方、一実施形態では、識別番号の長さは鍵長より長い。この場合、生成される鍵の鍵長ビットのLSBに対するモジュラ演算の効果が増し、その結果、共通鍵を生成しようとするデバイスペアにおいてそれらのビットが等しくならない可能性がある。しかし、対応する計算を行うときにより多くのビットが混合されるので、長い識別子を有することはセキュリティ面でポジティブな効果を有し得る。

【００５５】

多項式操作デバイスは、コンピュータ、例えば集積回路上で動作するソフトウェア内に実装され得る。多項式操作デバイスは、非常に効率的にハードウェア内に実装され得る。組み合わせも可能である。例えば、多項式操作デバイスは多項式を表現する係数のアレイを操作することによって実現されてもよい。

【００５６】

生成されたローカルキー材料をネットワークデバイスにおいて電子的に記憶することは、生成されたローカルキー材料を例えば有線接続又は無線接続を用いてネットワークデバイスに電子的に送信して、生成されたローカルキー材料をネットワークデバイスに保存することによって実行されてもよい。これは製造中又はインストール中、例えば、ネットワ

ークデバイス内の集積回路のテスト中に実行されてもよい。テスト機器はネットワーク権限を含んでもよいし、又はネットワーク権限に接続されてもよい。また、これは、デバイスが動作ネットワークに参加成功後に起こってもよい(すなわち、ネットワークアクセス又はブートストラッピング後) 。特に、ローカルキー材料は動作ネットワークパラメータの一部として送信されてもよい。

【００５７】

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ことは、ネットワークデバイスを鍵共有のために構成するためのシステム、例えばネットワーク権限デバイスからローカルキー材料を電子的に受け取ることによって実行され得る。また、ローカルキー材料の取得は、ローカルストレージ、例えばフラッシュメモリ等のメモリからローカルキー材料を引き出すことによって実行され得る。

【００５８】

第2のネットワークデバイスの識別番号を取得することは、識別番号を第2のネットワークデバイスから、例えば第2のネットワークデバイスから直接又は無線で受信することによって実行され得る。

【００５９】

公開モジュラス及び鍵モジュラスはネットワークデバイス内に記憶され得る。また、これらはネットワーク権限から受信されてもよい。また、これらはネットワークデバイスのソフトウェア内に暗示されてもよい。例えば、一実施形態では鍵モジュラスは2のべき乗である。かかる鍵モジュラスを法としたリダクションモジュロは、鍵長LSB以外の全てのビットを破棄することによって実行され得る。まず、代入の結果に公開モジュラスを法としたリダクションモジュロが行われ、その後、更に鍵モジュラスを法としたリダクションモジュロが行われる。

【００６０】

必須ではないが、公開モジュラス及び鍵モジュラスは互いに素でもよい。これは、公開モジュラスを奇数とし、鍵モジュラスを2のべき乗とすることによって達成され得る。いずれにせよ、公開モジュラスを法としたリダクションモジュロを省略することができ、鍵モジュラスが公開モジュラスを割ることを避けられる。

【００６１】

2つのデバイス間の鍵合意方法は、ルートキー材料として二変数多項式の数を使用し得る。xの機関間のxの合意をx変数多項式をルートキー材料として使用する鍵合意方法が用いられてもよい。この場合、TTPはx変数多項式を対応する環内の変数をもって評価し、得られたx－1 変数多項式はその後整数上で加算され、デバイスに記憶されるローカルキー材料を生成する。鍵についてxのデバイスが同意しなければならない場合、デバイスは、自身のローカルキー材料を他のx－1 のデバイスの識別子を用いて評価する。

【００６２】

ルートキー材料として非対称二変数多項式を使用すること、すなわち$f(x, y) \neq f(y, x)$は、第1のグループのデバイス及び第2のグループのデバイスが、それぞれ、デバイス上に記憶されるローカルキー材料KMである$KM(Id, y)$及び$KM(x, iD)$を受信する等、2つのデバイスグループの作成を可能にする。同じグループに属する2つのデバイスは共通鍵を生成することはできないが、異なるグループ内のデバイスは可能である。Blundoも参照されたい。

【００６３】

ネットワークデバイスの識別番号は、デバイスに関連付けられた情報を含むビット列の一方向関数として計算され得る。一方向関数はSHA2 又はSHA3 等の暗号ハッシュ関数であり得る。一方向関数の結果は、識別子のサイズに適合するよう切り捨てられてもよい。あるいは、一方向関数のサイズは最大識別子サイズより小さい。

【００６４】

一実施形態では、対称多項式は$\langle ax^i y^i \rangle_{pj}$の形式の単一の単項式を含み、ここで$\langle\rangle_p$はモジュール演算を表す。この場合、要素は有限群に含まれ、演算は乗算である。公開モジュ

ラスは秘密モジュラスより大きくても小さくてもよく、複数の秘密モジュラスが存在する場合、一部が公開モジュラスより大きく、一部が小さくてもよい。

【００６５】

ルートキー材料は任意の環にかけて評価され得る。Ax^a等の単一の単項式の多項式を使用することも可能であり、この場合、群が使用されてもよい。

【００６６】

本発明の一側面は、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（例えば、ネットワーク権限）に関連し、システムは、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、公開モジュラスのバイナリ表現及び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、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、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、生成されたローカルキー材料を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、多項式操作デバイスとを含み、二変数多項式に識別番号を代入し、代入の結果にリダクションモジュロパラメータセットの秘密モジュラスを行い、パラメータセットの二変数多項式から一変数多項式を決定することにより、少なくとも２つのパラメータセットそれぞれに関して対応する一変数多項式を取得して、各パラメータセットの公開モジュラス及び各パラメータセットの対応する一変数多項式を含む生成されたローカルキー材料をネットワークデバイスに電子的に保存するよう構成された生成部とを含む。

【００６７】

システムの一実施形態は、難読化数を生成するための難読化数生成部、例えば乱数生成部を含み、多項式操作デバイスは、難読化数を一変数多項式の係数に加えて難読化された一変数多項式を得るよう構成され、生成されたローカルキー材料は難読化された一変数多項式を含む。難読化数は、難読化多項式の係数として表現されてもよい。一実施形態では、難読化多項式の和の各係数は、２の鍵長乗の倍数である。一実施形態では、難読化多項式の和の各係数の２のべき乗による除算の商は、２の鍵長乗の倍数である。２のべき乗による除算は、整数への切り捨てによって計算されてもよい。

【００６８】

本発明の一側面は、共有鍵を決定するよう構成された第１のネットワークデバイスに関連し、鍵は暗号鍵であり、第１のネットワークデバイスは、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ためのローカルキー材料取得部であって、ローカルキー材料は少なくとも２つのオプションで難読化され得る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、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ための受信部と、オプションで難読化され得る少なくとも２つの一変数多項式のそれぞれに関して、第２のネットワークデバイスの識別番号を一変数多項式に代入し、代入の結果にリダクションモジュロ一変数多項式に対応する公開モジュラスを行い、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、リダクションモジュロ鍵モジュラスの結果から共有鍵を導出するための鍵導出デバイスとを含む。

【００６９】

鍵導出デバイスは、鍵モジュラスを法としたリダクションモジュロの結果から共有鍵を導出するよう構成されたコンピュータとして、例えば集積回路、実行ソフトウェア、ハードウェア、又はこれらの組み合わせとして実装され得る。

【００７０】

鍵モジュラスを法としたリダクションモジュロの結果から共有鍵を導出するステップとは、鍵導出関数、例えば、OMA DRM Specification of the Open Mobile Alliance (OMA-TS-DRM-DRM-V2_0_2-20080723-A, section 7.1.2 KDF)に規定される関数KDF等の関数の適用を含み得る。共有鍵の導出は、１つ以上のLSBを（鍵導出関数を適用する前に）破棄する

ことを含み得る。共有鍵を導出することは、更に、（鍵導出関数を適用する前に）整数を加算、減算、又は連結させることを含み得る。

【００７１】

それぞれが識別番号及び対応するローカルキー材料を有する複数のネットワークデバイスは、合わせて、ネットワークデバイスのペア間の安全な通信、例えば機密及び／又は認証通信のために構成された通信ネットワークを形成してもよい。

【００７２】

鍵生成はIDベースであり、デバイスペア間でペアワイズ鍵を生成することを可能にする。第１のデバイスAは、ローカルキー材料及び識別番号から鍵を導出するアルゴリズムに依拠し得る。

【００７３】

一実施形態では、第１のネットワークデバイスは第２のネットワークデバイスに鍵確認メッセージを送信する。例えば、確認メッセージはメッセージの暗号化を含んでもよく、更に、オプションでメッセージ自体を含んでもよい。第２のネットワークデバイスはメッセージの暗号化を検証し得る。送信の必要をなくすために、メッセージは固定で、第２のデバイスに存在してもよい。メッセージはランダム又はノンス等でもよく、この場合、暗号化と共に送信され得る。第２のデバイスは、鍵が合意するか否かの指標を含むメッセージをもって応答してもよい。また、第２のデバイスは自身の鍵確認メッセージをもって応答してもよい。第１及び／又は第２のデバイスが鍵が異なることを発見した場合、両者は、例えばLSBを削除する等によって鍵等化プロセスを開始し得る。

【００７４】

ネットワークデバイス及びシステムは電子機器であり得る。ネットワークデバイスはモバイルネットワークデバイスであり得る。

【００７５】

本発明に係る方法は、コンピュータ実行方法としてコンピュータ上に、専用ハードウェアとして、又は両者の組み合わせとして実装されてもよい。本発明に係る方法のための実行可能コードがコンピュータプログラム製品上に記憶されてもよい。コンピュータプログラム製品の例は、記憶装置、光学記憶装置、集積回路、サーバ、オンラインソフトウェア等を含む。好ましくは、コンピュータプログラム製品は、当該プログラム製品がコンピュータ上で実行されるとき本発明に係る方法を実行するためのコンピュータ読み取り可能媒体上に記憶される非一時的プログラムコード手段を含む。

【００７６】

好ましい一実施形態では、コンピュータプログラムは、コンピュータ上で実行されたとき、本発明に係る方法のステップを全て実行可能なコンピュータプログラムコード手段を含む。好ましくは、コンピュータプログラムはコンピュータ読み取り可能媒体上に具現化される。

【図面の簡単な説明】

【００７７】

本発明の上記及び他の側面は、後述される実施形態を参照して説明され、明らかになるであろう。

【００７８】

【図１】図１は、ルートキー材料生成部を示す概略的なブロック図である。

【図２】図２は、ローカルキー材料生成部を示す概略的なブロック図である。

【図３】図３は、通信ネットワークを示す概略的なブロック図である。

【図４】図４は、ローカルキー材料の生成を示す概略的なフローチャートである。

【図５】図５は、共有鍵の生成を示す概略的なフローチャートである。

【図６】図６は、共有鍵の生成を示す概略的なシーケンス図である。

【００７９】

異なる図において同じ参照符号を有する項目は、同じ構造的特徴及び同じ機能を有する、又は同じ信号である。かかる項目の機能及び／又は構造が説明されている場合、発明を

実施するための形態においてそれらを繰り返し説明する必要はない。
【発明を実施するための形態】
【００８０】
本発明は多様な実施形態を取り得るが、図面及び本明細書では、１つ以上の特定の実施形態が詳細に図解及び記述される。本開示は本発明の原理の例示として考えられるべきであり、本発明を図解及び記述される特定の実施形態に限定するものではないことを理解されたい。
【００８１】
以下、鍵共有方法の一実施形態が説明される。方法はセットアップフェーズ及び使用フェーズを有する。セットアップフェーズは開始ステップ及び登録ステップを含み得る。開始ステップはネットワークデバイスに関連しない。
【００８２】
開始ステップはシステムパラメータを選択する。開始ステップは信頼される第３者機関（TTP）によって実行され得る。しかし、システムパラメータは入力として与えられるとみなすこともできる。その場合、TTPはシステムパラメータを生成する必要はなく、開始ステップはスキップされ得る。例えば、TTPはデバイスメーカーからシステムパラメータを受け取ってもよい。デバイスメーカーが事前に開始ステップを実行してシステムパラメータを取得してもよい。説明の便宜上、TTPが開始ステップを実行するとするが、これは必須ではないことを留意されたい。
【００８３】
開始ステップでは、複数のパラメータセットが確立される。ネットワークデバイスの識別番号に基づき、パラメータセットを用いてローカルキー材料が生成される。各パラメータセットから、一変数多項式及び対応する公開モジュラスが取得される。ネットワークデバイスにはローカルキー材料は与えられるが、パラメータセットへのアクセスは与えられない。パラメータセットは新たなローカルキー材料の作成を可能にするため、信頼機関にしか知られず、一般的なネットワークデバイスには秘密にされる。
【００８４】
ネットワークデバイスＡは、自身のローカルキー材料及び異なるデバイスＢの識別番号から共有鍵を生成することができる。これを実行するために、ネットワークデバイスＡは自身のローカルキー材料を用いた計算を行う。
【００８５】
開始ステップ
開始ステップではルートキー材料が選択される。少数のパラメータはグローバルパラメータである。
【００８６】
使用フェーズ中にデバイス間で共有される鍵の望ましい鍵長が選択される（この鍵長を「b」とする）。低セキュリティアプリケーションのための典型値は64又は80であり得る。コンシューマレベルのセキュリティのための典型値は128であり得る。機密性が高いアプリケーションのためには、256以上の値が好ましい可能性がある。アルゴリズムのセキュリティ強度とｂとの間には直接の関係が無くてもよく、提供されるセキュリティは最大でｂである。システムを攻撃する将来のアルゴリズムによっては、アルゴリズムのセキュリティがｂより低い可能性がある。
【００８７】
生成されるパラメータセットの数が選択される（パラメータセットの数を「ｔ」とする）。ｔの高い値は、得られるシステムに対する攻撃、例えば格子ベース技術を用いた攻撃がより難しいことを示唆する。一方で、ｔのより高い値は、ネットワークデバイスにおけるより多くの計算及び保存の要求も示唆する。セキュリティが非常に低いアプリケーションのためにはｔ＝１の値が可能であるが、これは、十分な数の危殆化鍵が与えられれば、根本的な鍵材料が復元され得ることを示唆し得る。少なくともｔ＝２の値を取ることが推奨され、この値は既に、例えば格子ベース攻撃等の要求される暗号解読の複雑性を大きく

上昇させる。とはいえ、セキュリティが高いアプリケーションのためには、３、４、又は更に高い値さえ用いることができる。

【００８８】

次に、ｔ組のパラメータセットが選択される。各パラメータセットｊ（ｊ＝１，．．．，ｔ）は、所望の次数ａ、公開モジュラスＮ、少なくとも１つの秘密モジュラスp_1、及び少なくとも１つの対称二変数多項式f_1を含む。便宜上、公開モジュラスは自身が属するパラメータセットを示す下付き文字と共に記され得る（N_j）。

【００８９】

これらのパラメータを選択する好適な方法を以下に述べる。特に、各パラメータセットの二変数多項式はセキュリティセンシティブであり、通常のネットワークデバイスには開示されない。秘密モジュラスを開示する理由も存在しないので、これらは秘密にすることが推奨され、これらの知識はシステムに対する攻撃を容易にする可能性さえある。鍵長ｂ及び公開モジュラスN_jはネットワークデバイスにおいて必要であり、信頼機関だけの秘密にすることはできない。

【００９０】

各パラメータセットは潜在的な難問の難しさに寄与する。後述されるように、一部のパラメータの選択は、他の選択よりも難しい問題を生じさせる。原則的に、パラメータセットの選択は独立であり、例えば、より高いセキュリティに対応する値を有する１つのパラメータセットを選択して、より小さいパラメータを有する第２のセットを選択してもよい。この場合、第２の及び／又は更なるセットは主に難しいセットに対する攻撃を防ぐことに寄与する。このシナリオでは、セキュリティの境界（bounds）を導き出すのがいくらか容易な可能性がある。一方で、全て同等な難しさのパラメータセットを選択してもよい。後者の場合、問題の難しさは全てのセットに由来する。これは、ネットワークデバイスにおける計算資源を最適化する。

【００９１】

パラメータセット選択ステップ

これらのステップは、所望のパラメータセットごとに一度ずつ、ｔ回繰り返される。

【００９２】

多項式の次数を制御する望ましい次数が選択される（次数を「ａ」とする（$1 \leq a$））。ａの実践的な選択は2である。セキュリティがより高いアプリケーションはより高いaの値、例えば3若しくは4、又はそれ以上さえ使用し得る。単純なアプリケーションのためにはa=1も選択可能である。a=1のケースはいわゆる「hidden number problem」に関連し、より高い「ａ」の値はノイジー多項式補間問題に関連し、これらのケースが破られにくいことを保証する。

【００９３】

多項式の数が選択される。多項式の数は「ｍ」とする。ｍの実践的な選択は２である。セキュリティがより高いアプリケーションはより高いｍの値、例えば３若しくは４、又はそれ以上さえ使用し得る。高いｍの値はＴＴＰにおけるより高い実装複雑性を暗示するため、複雑性の低いアプリケーションは低いｍの値を課し得ることに留意されたい。

【００９４】

高いセキュリティパラメータａ及びｍの値は、システムの複雑性、よってそのIntractability（手に負えなさ、処理しにくさ）を高める。複雑なシステムほど解析が困難になるので、暗号解読に対して高い耐性を持つ。次数ａは好適に全てのパラメータセットで同じでもよく、ｍも全てのパラメータセットで同じでもよいが、これは必須ではないことに留意されたい。

【００９５】

一実施形態では、$2^{(a+2)b-1} \leq N$を満たし、最も好ましくは更に$N \leq 2^{(a+2)b}-1$を満たす公開モジュラスＮが選択される。この制限は厳密に必要ではなく、システムはより小さい／大きい値のＮを使用することもできるが、最良の選択肢であるとは考えられない。

【００９６】

鍵長、多項式の次数、及び多項式の数は、例えばシステム設計者によってしばしば事前に決定され、TTPに入力として提供される。実践的な選択として、$N=2^{(a+2)b}-1$が選択され得る。例えば、a=1、b=64の場合、Nは$N=2^{192}-1$であり得る。例えば、a=2、b=128の場合、Nは$N=2^{512}-1$であり得る。Nについて上記区間の上限又は下限を選択することは、計算を簡単にするという利点を有する。攻撃者にとっての複雑性を高めるために、範囲内の乱数をNとして選択してもよい。

【００９７】

信頼できる第３者機関（TTP）によってm個の秘密モジュラス$p_1, p_2, \ldots, p_m$が選択される。秘密モジュラスは正の整数である。各デバイスは登録ステップ中に識別番号と関連付けられる。選択される各秘密モジュラスは、使用される最大の識別番号より大きい。例えば、識別番号が2^{b-1}以下且つ選択秘密モジュラスが2^{b-1}より大きいことを要求することによって識別番号を制限してもよい。選択される各数値は関係$p_j=N+\gamma_j \cdot 2^b$を満たす。ここで、γ_jは$|\gamma_j|<2^b$であるような整数である。この条件を満たす数値を選択する実践的な方法の一例は、$-2^b+1 \leq \gamma_j \leq 2^b-1$であるようなm個のランダムな整数$\gamma_j$のセットを選択し、関係$p_j=N+\gamma_j \cdot 2^b$から選択秘密モジュラスを計算する方法である。$|\gamma_j|$をもう少し大きくすることも許容されるが、モジュラ演算が行き過ぎ、共有鍵が等しくならないという問題が起こり得る。

【００９８】

m>1の場合、モジュラスが異なるモジュロ演算が、かかる演算は通常の数学的意味では両立しないにも関わらず、組み合わせられるので、システムはより複雑であり、よってよりセキュアである。したがって、ペアワイズに異なるように選択秘密モジュラスを選択することは有利である。

【００９９】

次数a_jの対称二変数多項式$f_1, f_2, \ldots, f_m$がm個生成される。全ての次数が$a_j \leq a$を満たし、最も好ましくはa=MAX{$a_1, \ldots, a_m$}である。実践的な選択肢は、それぞれが次数aの多項式となることである。二変数多項式は変数が２つの多項式である。対称多項式fは$f(x, y)=f(y, x)$を満たす。各多項式f_jが、モジュロp_jを計算することによって得られる整数モジュロp_jによって形成される有限環において評価される。整数モジュロp_jは、p_jの元を含む有限環を形成する。一実施形態では、多項式f_jは０からp_j-1までの係数によって表される。二変数多項式はランダムに、例えば、これらの制限内でランダムな係数を選択することによって選択され得る。

【０１００】

これらの二変数多項式はシステムのルートキー材料であり、よって鍵共有のセキュリティは二変数多項式に依存する。したがって、これらを保護するために強力な手段、例えば制御手順、耐タンパーデバイス等が取られることが好ましい。p_jに対応するγ_jの値を含め、選択された整数$p_1, p_2, \ldots, p_m$も秘密にされることが好ましいが、重要性はより低い。二変数多項式は次の形式でも記載される（j=1, 2, ..., m）。

$$f_j(x,y)=\sum_{i=0}^{a} f_{i,j}(x)y^i$$

【０１０１】

上記実施形態は多様に変更できる。公開及び秘密モジュラスに対する制限は、一変数多項式の難読化が可能であるが、ネットワークデバイスにおいて得られる共有鍵が依然として十分な頻度で十分に互いに近いよう、多様に選択され得る。上記のように、何をもって十分とするかはアプリケーション、要求されるセキュリティレベル、及びネットワークデバイスにおいて利用可能な計算資源に依存する。上記実施形態は、多項式シェアが整数上で加算されるとき、多項式シェアの生成時に実行されるモジュラ演算が非線形に組み合わせられるよう正の整数を組み合わせ、ネットワークデバイス上に記憶されるローカルキー材料の非線形構造を作成する。N及びp_jの上記選択は、次の特性を有する：（ｉ）Nのサイ

ズは全てのネットワークデバイスについて固定であり、aに関連する、（ii）非線形効果は、デバイス上に記憶される鍵材料を形成する係数の最上位のビット（most significant bits; MSB）に現れる。その特定の形式のため、共有鍵は、リダクションモジュロNの後にリダクションモジュロ2^bを行うことによって生成されてもよい。

【０１０２】

これらのデザインコンセプトは、前段落で述べたような特徴（i）及び（ii）を改良するために、より一般的に適用され得る。以下に公開及び秘密モジュラスを選択する異なる一般的構成が与えられる。第１の点（i）に取り組むために、N及びp_jのためのこの構造は、$p_j=2^X+\gamma_j 2^{Y_j}-1$と記載する場合、より一般的な式に適合する（各jについて、$Y_j+b\alpha_j=X$且つ$|\gamma_j|<2b$）。この式は、非線形効果を導入するときに最大の効果を保証する一方、より可変な形式のp_jを可能にする。$Y_j+b\alpha_j \fallingdotseq X$としてもよく、ここで左辺と右辺の差は鍵長の端数である。

【０１０３】

第２の点（ii）に取り組むために、N及びp_jに関する上記形式は、$p_j=\beta 2^X+\gamma_j 2^{Y_j}+\zeta_j 2^{Z_j}$という更に一般的な式に適合する。例えば、$\zeta_j=-1$、$\beta=1$且つ$Z_j=0\ \forall j$と設定することにより、異なる$\gamma_j$値がネットワークデバイス上に記憶される鍵材料の係数のMSBに非線形効果をもたらす前記式が得られる。この場合、定数である公開モジュラス（N）は$N=2^X-1$であり、モジュラ演算に関与する異なる正の整数の生成に使用される秘密可変部分は$\gamma_j 2^{Y_j}$である。あるいは、$\gamma_j=1$、$\beta=1$、$Z_j=0$、$Y_j=(\alpha_j+1)b$、$X=(\alpha_j+2)b\ \forall j$と設定してもよく、ここで、$\zeta_j$は$|\zeta_j|<2b$であり、jごとに異なる。この場合、$\zeta_j$の違いがノード上に記憶されるローカルキー材料の係数の最下位のビット（LSB）に非線形効果をもたらすことを可能にする。この場合は公開部分、すなわち一定のままの部分の構成も異なり、$N=\beta_j 2^{Xj}+\gamma_j 2^{Yj}=2^X+2^{b(\alpha j+1)}$である。この場合、非線形効果は最下位の部分にあり、前述の最大混合効果のための条件のため、差$Y_j-Z_j-\log_2(\zeta_j)$は$\alpha_j b$でなければならない。同様に、同じ概念に基づいて他の構成を定めることも可能である。

【０１０４】

上記したように、パラメータのための多数の選択が可能である。しかし、一部の選択肢はより優れた実装形態を与える。特に公開モジュラスの選択は重要である。例えば、公開モジュラスの一部の選択肢は効率的なモジュロ演算を可能にする。また、鍵が取得されるビット、例えばＬＳＢに対する公開モジュラスの効果は異なることが好ましい。異なる効果は、共有鍵を生成するための演算を実行し、p_iの違いが異なる鍵生成方法をもたらすか否かをテストすることによって試行されてもよい。これは以下の例にて見ることができる。

【０１０５】

例えば、鍵長の数のLSBにおける差が小さい、例えば所定の差未満の公開モジュラスを選択することは好適である。例えば、一実施形態はt=2、$N_1=2^{(a+2)b}-1$、及び$N_2=2^{(a+2)b}-2-1$等の数を選択し得る。この具体例では、リダクションモジュールN_1が－２の項の効果を含まない一方、リダクションモジュールN_2はそれを含むため、鍵生成フェーズ中に-2の項が重要な役割を果たす。この場合、リダクションは$(\alpha+2)b$ビットより高いオーバーフロービットを最下部に移動させることに関することに留意されたい。

【０１０６】

しかし、このようにして公開モジュラスを選択することの問題は、2^bよりはるかに小さい限られた数の選択肢しか利用できないことである。一般的に、h<b且つh>1であるような項2^hをNに導入することが望まれる。また、Nの異なる形式によって実際に影響を受けるビット数は約b-hであり、約2^hの異なる数しか存在しないことも問題である。これらの問題を克服するために、例えば、Nの選択肢を増やし、異なる演算の影響を受ける鍵のために使用可能なビット数を最大化するために、２つ前の段落の態様でp_iのより一般的な定義を使用してもよい。その場合、例えば$p_i=N-\gamma_i 2^{b(a+1)}-\zeta_i$を対応する公開モジュラス$N=2^{(a+2)b}-2^{ba}$と共に使用することにより、多項式係数のMSB及びLSBの両方に非線形効果が導入される。本明細書で定められるように、全てのp_iに対して異なるγ_i及びζ_iが選択され、

また、好ましくは全パラメータセットにわたり異なる。この場合、鍵はLSBからではなく中央のビットから生成される。

【０１０７】

類似の選択は以下の通りである。これらの等式において、第1 のインデックスiはパラメータセットを示し、tまでのぼり、第2 のインデックスjはパラメータセットごとに使用される数pの番号を示し、mまでのぼる。

$$N_i = 2^{(a+2)b} - 2^{ba} - \zeta_i$$

$$p_{i,j} = N_i - \gamma_{i,j} 2^{b(a+1)}$$

【０１０８】

実践的な選択は、t=2を取ることである。その後、各パラメータセットが選択され得る。実践的な選択は、各パラメータセットについてm=2を取ることである。特に直前の等式では、これらは良い選択である。この構成によれば、bビットのζ値を例えばランダムに変更することにより、多くのN_iを見つけることができる。この構成では、$\gamma_{i,j}$パラメータはデバイス上に保存される鍵材料シェアの生成において混合を実行する。これは信頼機関によって行われ得る。ζパラメータは、デバイス上で鍵の混合を実行する。最も好ましくは、上記実施形態と同じ動機に従い、この場合においてもノイズが加えられる。この場合、鍵が抽出される位置（すなわち中央のビット）においてノイズ、すなわち難読化多項式の和がゼロになるよう、ノイズのための条件を更新しなければならない。

【０１０９】

公開モジュラス、例えばN_1及びN_2が全て2^bの倍数ではないことが好ましい。これは、正の整数a、m n及び適切な整数qに対して、a=qmn+<a>$_{mn}$、よってa≡<a>$_{mn}$ mod nが成立し、<a>$_n$=<<a>$_{mn}$ >$_n$が推定されるからである。結果として、N_1及びN_2が共に2^bの倍数の場合、

$$\langle\langle F_\eta^1(\eta')\rangle_{N_1} + \langle F_\eta^2(\eta')\rangle_{N_2}\rangle_{2^b} = \langle F_\eta^1(\eta') + F_\eta^2(\eta')\rangle_{2^b}$$

である。すなわち、問題はt=1のケースに下がる。

【０１１０】

登録ステップ

登録ステップでは、各ネットワークデバイスに鍵材料（KM）が割り当てられる。ネットワークデバイスは識別番号に関連付けられる。識別番号は、例として、オンデマンドで、例えばTTPによって割り当てられてもよいし、又はデバイス内に予め記憶されていてもよく、例えばメーカー側においてデバイス内に記憶されてもよい。

【０１１１】

TTPは、以下のようにt の多項式を計算することにより、識別番号A のデバイスのための鍵材料のセットKM^を以下のようにして生成する。

$$F_i^A(X) = \sum_{j=1}^{m} < f_j(x,A) >_{p_j} + \sum_{k=0}^{a} \epsilon_{i,k}^A X^k = \sum_k C_{i,k}^A X^k$$

【０１１２】

上式において、インデックスiはパラメータセットを示し、つまり1からtまでのぼる。インデックスjはパラメータセットごとの多項式及び秘密モジュラスの数を示す。インデックスkは難読化多項式内の係数を示す。パラメータセットごとに1 つの難読化多項式が選択されることに留意されたい。パラメータセットの一部又は全てが難読化多項式を有さなくてもよい。また、上記一変数多項式に対応するパラメータセットからの公開モジュラスがローカル鍵材料に含まれる。

【０１１３】

Xは仮変数である。鍵材料は非線形であることに留意されたい。<・・・>$_{p_j}$という表記は、括弧内の多項式の各係数モジュロp_jを表す。表記「$\varepsilon_{A,i}$」は

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

.

であるようなランダムな整数(難読化数の一例) を表す。ランダムな整数はいずれも正でも負でもよい。乱数εはやはりデバイスごとに生成される。したがって、項

$$\sum_{k=0}^{a} \epsilon_{i,k}^{A} X^{k}$$

はiごとのa次のXの多項式を表し、係数長は次数が高いほど小さい。あるいは、より一般的ではあるがより複雑な条件は、

$$\sum_{k=0}^{a} |\epsilon_{i,k}^{A}| \cdot 2^{b+k}$$

が小さい、例えば<2aである。

【０１１４】

全ての他の加算は普通の整数演算を使用してもよいし、又は(好ましくは) 加算モジュロ(アディションモジュロ) Nを使用してもよい。したがって、一変数多項式

$$\sum_{j=1}^{m} < f_j(x, A) >_{p_j}$$

の評価は、それぞれ、モジュロより小さいモジュラスp_jによって個別に行われるが、これらのリダクション一変数多項式自体の総和は、好ましくはモジュロNによって行われる。また、難読化多項式

$$\sum_{k=0}^{a} \epsilon_{i,k}^{A} X^{k}$$

の加算も通常の整数演算を用いて行われてもよいし、又は、好ましくはモジュロNによって行われてもよい。鍵材料は係数

$$C_{i,k}^{A}$$

(k=0, . . . , a、i =1, . . . , t) を含む。鍵材料は上記のような多項式のセットとして示され得る。実際には、鍵材料は整数

$$C_{i,k}^{A}$$

のリスト、例えば二次元アレイとして記憶されてもよい。デバイスAは更に数値N及びbも受信する。多項式の操作が行われてもよく、例えば係数を含むアレイの操作として、例えば全係数を所定の順番に並べてもよい。多項式は他のデータ構造、例えば、(次数, 係数) ペアの集合を、好ましくは集合内に各係数が最大で一度現れるよう含む連想配列(又は「マップ」) として実現されてもよい。デバイスに提供される係数

$$C_{i}^{A}$$

は好ましくは0, 1, . . N-1の範囲内である。識別子のサイズが小さいため、係数の全てのビットが鍵生成のために使用されない可能性がある。その場合、関連する係数部分のみを保存すればよい。

【０１１５】

本明細書の始めに示されるように、デバイスAが相手方のデバイスBと異なる共有鍵を導き出す可能性を下げるために、難読化多項式は各k ＝0, . . . , aに対して次式が成立するよう選択され得る。

$$\sum_{i=1}^{t} \varepsilon_{i,k} \equiv 0 \bmod 2^b$$

【０１１６】

すなわち、全ての難読化多項式の和は2^bの倍数である。上述したように、これは、攻撃者が鍵材料を加算することによりノイズを除去しようとする場合、モジュラスが異なるモジュロ演算を実行することによって得られた鍵材料を混合することになるという良好な特性を有する。これらを加算しなければ、鍵材料はノイズによって隠される。

【０１１７】

N及び整数p_jに関するより一般的な構成が使用される場合、乱数εが係数の異なる部分に作用するよう難読化多項式を適合しなければならない。例えば、非線形効果がネットワークデバイス上に記憶される鍵材料の係数のLSB内に導入される場合、乱数は係数の最上位の部分、及び係数の最下位の部分の可変ビット数にのみ影響を及ぼすべきである。これは上記方法の直接的拡張であり、他の拡張も実行可能である。

【０１１８】

使用フェーズ

２つのデバイスA及びBが識別番号を得て、TTPから各自の鍵材料を受信した後、両デバイスは鍵材料を用いて共有鍵を取得できる。デバイスAは以下のステップを実行して自身の共有鍵を取得し得る。まず、デバイスBはデバイスBの識別番号Bを取得して、続いて以下の式を計算することによって共有鍵を生成する。

$$K_{AB} = < \sum_i < F_i^A(X)|_{X=B} >_{N_i} >_{2^b} = < \sum_i < \sum_k C_{i,k}^A B^k >_{N_i} >_{2^b}$$

【０１１９】

つまり、Aは、自身の鍵材料からの自身の各一変数多項式

$$F_i^A$$

を値Bについて評価する。鍵材料の評価の結果は整数である。次に、デバイスAは評価の結果をまず対応する公開モジュラスN_iを法としたモジュロによってリダクションする。次に、モジュロ評価後の全ての多項式

$$F_i^A$$

の評価結果が整数として加算され、続いて鍵モジュラス2^bを法としたモジュロによってこの総和の結果をリダクションする。結果はAの共有鍵と呼ばれる０から2^b-1の整数である。デバイスBにおいては、デバイスBは自身の鍵材料を識別子Aについて評価して、結果をモジュロN及び続いてモジュロ2^bによってリダクションすることにより、Ａと同様な態様でBの共有鍵を生成できる。

【０１２０】

上記に則して、N及び正の整数p_jのより一般的な式が使用される場合、bビットの鍵の取得方法に小さい適合を加えなければならない。特に、秘密モジュラスとして

$$p_{i*m+j} = \beta 2^X + \gamma_{i*m+j} 2^{Y_{i,j}} + \delta 2^W + \zeta_i 2^{Z_i}$$

が、公開モジュラスとして

$$N_i = \beta 2^X + \delta 2^W + \zeta_i 2^{Z_i}$$

が取られ、これは、bビットの項$\gamma_{i\cdot m+j}$により、鍵材料シェア内に非線形を導入することを可能にする。この特定の構成では、各鍵材料セット内にm個の多項式があり、各多項式が識別子jによって示されることに留意されたい。更に、iによって示される最大でt組の

異なる鍵材料セットを有し得る。また、$Y_{i,j}$は典型的には一定（$\forall i,j$）であることに留意されたい。更に、bビットの項ζ_iはN_i（$i=1,\ldots,t$）ごとに異なり、ノード上で異なる鍵材料から生成された鍵を混合するとき、非線形効果を導入する。このケースでは、鍵は次のようにして生成される。

$$K_{AB} = < \frac{\sum_i \; < F_i^A(X)|_{X=B} >_{N_i}}{2^W} >_{2^b}$$

【０１２１】

上記されるように、tの鍵材料シェアはそれぞれx=Bにおいて評価され、モジュラスN_iによってリダクションされる。このリダクションにおいて、ζ_iの効果が導入される。全ての$p_{i \cdot m+j}$に共通の最小の２の乗数はwなので、共通鍵が生成され得るよう、結果が2^wによって除算（整数除算）される。

【０１２２】

ルートキー材料の二変数多項式は対称なので、Aの共有鍵及びBの共有鍵は、必ずしも常にではないが、等しい。パラメータセット内の秘密モジュラス、整数p_1，p_2，．．．，p_m、及び乱数εに関する特定の条件は、モジュロ２の鍵長乗後の鍵がしばしば互いに等しく、ほとんどの場合近いようなものである。A及びBが同じ共有鍵を取得した場合、両デバイスはそれをA及びB間で共有される対称鍵として使用し、例えば様々な暗号アプリケーションのために使用し、例えば共有鍵を用いた１つ以上の暗号及び／又認証メッセージを交換し得る。好ましくは、マスター鍵の更なる保護のために共有鍵に鍵導出アルゴリズムが適用され、例えば、ハッシュ関数が適用され得る。

【０１２３】

A及びBが同じ共有鍵を取得しなかった場合、これらの鍵はほぼ確実に互いに近似であり、両鍵の複数のLSBを除去することにより、ほぼ常に鍵を同じにすることができる。A及びBは鍵確認を実行することによって両者の共有鍵が等しいか否かを検証でき、例えば、AはBにペア（m　E(m)）を含むメッセージを送信してもよく、ここでmは例えば固定文字列又は乱数等のメッセージであり、E(m)はAの共有鍵を用いたその暗号化である。

【０１２４】

E(m)をBの共有鍵を用いて解読することにより、Bは両鍵が等しいか否かを検証できる。鍵が等しい場合、BはAに状況を知らせることによって応答してもよい。

【０１２５】

鍵が等しくない場合、A及びBは鍵等化プロトコルに従事してもよい。例えば、両デバイスは２つの鍵が算術的に互いに近いという事実を利用してもよい。例えば、ネットワークデバイスA及びBは、鍵が等しくなるまで、LSBを除去して鍵確認メッセージを送信することを繰り返してもよい。同じ鍵を得た後、A及びBは鍵導出アルゴリズムを使用して通常の鍵長の鍵を再取得してもよい。

【０１２６】

選択されるm個の秘密モジュラスp_1，p_2，．．．，p_mは、好ましくはペアワイズに互いに素である。これらの数字がペアワイズに互いに素である場合、モジュロ演算間の両立性の無さが増す。ペアワイズに互いに素である数字の取得は、整数を順に選択し、各数字の全ペアが依然として互いに素であるか否かを新たな整数ごとにテストして、そうでない場合、直前に選択された数字をセットから除去することによって実現され得る。この手順はm個の数字全てが選択されるまで続く。

【０１２７】

選択されるm個の秘密モジュラスp_1，p_2，．．．，p_mが異なる素数であることを要求することによって複雑さは更に増す。この場合、各素数は形式$p_j = N + \gamma_j \cdot 2b$を有することを要求され得る。ここで、$\gamma_j$は$|\gamma_j| < 2^b$であるような整数である。実験により、これらの素数が容易に得られることが確認された。例えば、素数が見つかるまで、ランダムなγ_jを選択して求められたp_jをテストすることを繰り返してもよい。上記のようなより一般的な式が適用される場合でも同様である。実際に、これは、aのオーダーがbと大体同じであり

、特にa<bである限り、かかる素数は豊富であるという算術級数の素数定理に則る。特に、64、128、196、256のグループ内の鍵長と2、3のグループ内の次数のあらゆる組み合わせに関しては、実験により、上記アルゴリズムを使用してこの形式の素数を実践的な制限時間内に多数生成できることが確認された。素数を用いる場合、各多項式f_jはp_j個の元を含む有限体においてこのように選択される。

【０１２８】

登録及び使用フェーズ中に使用される様々なパラメータの選択について、多くの変形形態が可能である。例えば、単純化された実施形態では秘密モジュラスが公開モジュラスより小さく、関係$p_j=N-\beta_j \cdot 2^b$を満たす。ここで、β_jは$\beta_j<2^b$であるような正の整数である。この条件を満たす数字を選択する１つの実践的な方法は、$\beta_j<2^b$であるようなm個のランダムな正の整数β_jのセットを選択し、関係$p_j=N-\beta_j \cdot 2^b$から選択秘密モジュラスを計算するという方法である。

【０１２９】

上記したように、差$Y_j-Z_j-\log_2(\zeta_j)$はα_j bであり得る。同様に、同じ概念に従って他の構成が定められてもよい。特に、秘密モジュラスは$p_j=\beta 2^X+\gamma_j 2^{Yj}+\delta 2^W+\zeta_j 2^{Zj}$と、公開モジュラスは$N=\beta 2^X+\delta 2^W$と記載され得る。この構成の特定の一具体化は、$p_j=2^{2(a+1)b}+\gamma_j 2^{(a+1)b}+2^{ab}+\zeta_j$及び$N=2^{2(a+1)b}+2^{ab}$である。この場合、項$\gamma_j$及び$\beta_j$の絶対値は$2^b$より小さく、デバイス上に記憶されるローカルキー材料の係数のMSB及びLSBに対する非線形効果を作り出す役割を果たす。デバイスの識別子の長さは約bビットなので、γ_j（β_j）は、整数モジュロp_jの環において評価される多項式シェアの係数のMSB（LSB）に影響を与えることに留意されたい。その後、デバイスのローカルキー材料の生成中、異なる環内の多項式シェアの係数が整数上で加算されることによって寄与の起源が隠される。

【０１３０】

鍵は

$$K_{AB}=<\frac{\sum_l <F_l^A(X)|_{X=B}>_{N_l}}{2^W}>_{2^b}$$

のようにして生成され得るが、MSB及びLSBの両方に非線形効果を導入することを可能にするp_j及びNの更に一般的な式が使用される場合、リダクションモジュロN後の除算は２のW乗により、ここで2^Wは、Nが整数倍である最も高い２の整数乗である。N及びp_jの他の構成は、異なる２のべき乗による除算を要求し得る。ルートキー材料内の二変数多項式は対称なので、Aの共有鍵及びBの共有鍵は、必ずしも常にではないが、しばしば等しい。

【０１３１】

図１は、ルートキー材料生成部１００を示す概略的なブロック図である。鍵材料取得部は、ローカルキー材料生成部がローカルキー材料を生成するために必要とする入力データ（識別番号を除く）を提供するよう構成される。鍵材料取得部の一例は鍵生成部である。入力データの全て又は一部を生成する代わりに、一部のパラメータはルートキー材料生成部がそれらを受信することによって取得されてもよい。例えば、鍵取得部は入力データ、例えば公開及び秘密モジュラスを受信するための電子受信機を備えてもよい。鍵材料取得部は、識別番号を除く全ての必要なパラメータを外部ソースから取得する。一実施形態では、a、b、mは既定であり、例えば受信され、パラメータセット内の公開モジュラス及び秘密モジュラス、並びに対応する（対称）二変数多項式は生成される。一実施形態では、公開モジュラスも既定であり、例えば受信される。

【０１３２】

ルートキー生成部１００は複数のパラメータセットを生成し、生成しなければならないパラメータセットの数を有するパラメータセット数t 要素１３０を含む。例えば、t=2又はt=3等である。

【０１３３】

ルートキー生成部１００は、所与のパラメータセットに対して、多項式次数、鍵長、及び多項式の数、すなわちa、b、及びmをそれぞれ提供（供給）するよう構成された多項式

次数要素１１２、鍵長要素１１４、及び複数の多項式要素１１６を備える。典型的には、鍵長要素１１４は全てのパラメータセットにわたり同じである。典型的には、多項式次数要素１１２も全てのパラメータセットにわたり同じであるが、これは必須ではない。一部の実施形態では、多項式数要素１１６はパラメータセットにわたり変更され、例えば、あるものがm=1を使用する一方、あるものはm=2を使用し得る。mを全てのセットにわたり一定に、例えばm=1又はm=2とすることも可能である。

【０１３４】

例えば環境によってはこれらの要素は生成されてもよいが、典型的にはこれらのパラメータはシステム設計者によって選択される。例えば、要素は不揮発性メモリとして、要素の値を受信するための受信機として、又は受信機に接続される揮発性メモリ等として設計され得る。適切な選択はｔ＝２、a=2、b=128、m=2を含む。よりセキュリティの高い又は低いシステムを得るために、これらの値のいずれかをより高く又は低くしてもよい。

【０１３５】

ルートキー生成部１００は、パラメータセットの公開モジュラスNを提供するよう構成される公開モジュラス要素１１０を含む。公開モジュラスはシステム設計者によって選択されてもよいし、そうでなくともよい。例えば、公開モジュラスは、速いリダクションを可能にする好都合な数字に設定され得る（２のべき乗に近い又は２のべき乗）。公開モジュラスは要素１１２及び１１４によって決定される範囲内で選択される。

【０１３６】

ルートキー生成部１００は、秘密モジュラスp、又は複数の秘密モジュラス$p_1, \ldots, p_m$を提供するよう構成される秘密モジュラスマネージャー１２２を含む。例えば、秘密モジュラスは適切な制限内でランダムに選択される。

【０１３７】

ルートキー生成部１００は、対称二変数多項式f、又は複数の対称二変数多項式$f_1, \ldots, f_m$を提供するよう構成される対称二変数多項式マネージャー１２４を含む。対称二変数多項式は、それぞれ、対応する秘密モジュラス（すなわち、同じインデックスを有する秘密モジュラス）を法とした係数ランダムモジュロによって選択される。係数は0からp-1の範囲内で選択され、ランダムで選択され得る。

【０１３８】

秘密モジュラスは、公開モジュラスに／から２の鍵長乗の倍数を足す／引くことによって選択され得る。これは、公開モジュラスとの差が連続する０で終わるような秘密モジュラスをもたらす。また、鍵長の連続０が末部ではなく、LSBから数えて他の位置、例えば位置「s」に現れるように公開モジュラス及び1つ以上の秘密モジュラスを選択してもよい。

【０１３９】

図１’は、ルートキー生成部１００によって生成されるルートキー材料１８０の一例を示す。ルートキー材料１８０はパラメータセットの数１４０を含み、この場合は値３を有する。ルートキー材料１８０は３組のパラメータセットを含む。第１のセットは公開モジュラス１４１、秘密モジュラス１５１、１５３、及び１５５、並びに対応する二変数多項式１５２、１５４、及び１５６を含む。第２のセットは公開モジュラス１４２、秘密モジュラス１６１及び１６３、並びに対応する二変数多項式１６２及び１６４を含む。第３のセットは公開モジュラス１４３、秘密モジュラス１７１、１７３、及び１７５、並びに対応する二変数多項式１７２、１７４、及び１７６を含む。このケースでは多項式の次数は多項式の表現内で暗示されるが、明示されてもよい。このルートキー材料１８０の例では、鍵長１４４も記録される。

【０１４０】

動作中、ルートキー材料取得部１００は、要素１３０における数に等しい数のセットが生成されるまで、パラメータセットを繰り返し生成する。パラメータセットの数はルートキー材料１８０内の１４０に記録されてもよい。

【０１４１】

図２は、ローカルキー材料生成部２００を示す概略的なブロック図である。鍵材料生成部１００及びローカルキー材料生成部２００は、合わせて、鍵共有のためにネットワークデバイスを構成するシステムを形成する。

【０１４２】

ローカルキー材料生成部２００は多項式操作デバイス２４０を含む。ローカルキー材料生成部２００は、多項式操作デバイス２４０にルートキー材料を提供するための、すなわち、多項式操作デバイス２４０に複数のパラメータセットを提供し、よって複数の一変数多項式を生成するためのルートキー材料要素２１０を含む。要素２１０は鍵材料生成部１００の対応する要素によって実現され、また、これらの要素は鍵材料生成部１００に接続されるメモリ又はバスであり得る。

【０１４３】

ローカルキー材料生成部２００は、多項式操作デバイス２４０に難読化数「$\varepsilon_{A,i}$」を提供するための難読化数生成部２６０を含む。難読化数は、例えば乱数生成部によって生成される乱数であり得る。難読化数生成部２６０は、一変数多項式の複数の係数に対して複数の難読化数を生成し得る。生成部２６０は単一の数、例えばパラメータセットごとに１つの難読化数又は少なくとも２つのパラメータセットのために１つの難読化数を生成するよう制限されてもよいが、生成部２６０は、難読化された一変数多項式を得るために現在のパラメータセットに対応する一変数多項式に加えられる非ゼロ難読化多項式を生成するよう構成されてもよい。一実施形態では、一変数多項式の係数ごとに難読化数が決定される。難読化多項式は１、２、又はそれ以上の非ゼロ係数を有し得る。

【０１４４】

ローカルキー材料生成部２００は、ローカルキー材料が生成されるべき識別番号を例えばネットワークデバイスから受信し、ローカルキー材料をその識別番号に対応するネットワークデバイスに送信するよう構成されるネットワークデバイスマネージャー２５０を含む。識別番号を受信する代わりに、例えばランダム、シリアル、又はノンス番号として識別番号を生成してもよい。後者の場合、ローカルキー材料と共に識別番号がネットワークデバイスに送信される。

【０１４５】

多項式操作デバイス２４０は、ルートキー材料要素２１０内のパラメータセットごとに一変数多項式を生成する。

【０１４６】

多項式操作デバイス２４０は、パラメータセットごとに、マネージャー２５０からの識別番号を各二変数多項式に代入し、それぞれを対応する秘密モジュラスを法としたモジュロによってリダクションする。得られた複数のリダクション一変数多項式は、普通の算術加算によって係数的に加算される。また、１つ以上の難読化数が足される。好ましくは、結果が、やはり係数的に、公開モジュラスを法としたモジュロによってリダクションされる（係数は0からN-1の範囲内で表され得る）。

【０１４７】

難読化された一変数多項式は、識別番号に対応するローカルキー材料の一部である。必要な場合、公開モジュラス、次数、及び鍵長もネットワークデバイスに送信される。

【０１４８】

図２’は、ルートキー材料１８０からネットワークデバイスのために生成されたローカルルートキー材料２８０を示す。ローカルルートキー材料２８０は、パラメータセットの数１４０（ここでは３）、鍵長１４４、公開モジュラス１４１、１４２、及び１４３、並びに対応する生成された（難読化されていてもよい）一変数多項式２５２、２６２、及び２７４を含む。オプションで、ローカルルートキー材料２８０は除算のための２のべき乗、及び共有鍵を生成するための鍵モジュラスを含んでもよい。

【０１４９】

図３は、複数のネットワークデバイス（図示されているのは第１のネットワークデバイス３１０及び第２のネットワークデバイス３２０）を含む通信ネットワーク３００を示す

概略的なブロック図である。第１のネットワークデバイス３１０について説明する。第２のネットワークデバイス３２０は同じでもよいし、又は同じ原理に従って動作し得る。

【０１５０】

ネットワークデバイス３１０は、第２のネットワークデバイスと有線又は無線で電子形式、例えばデジタル形式のメッセージを送受信するための送信機及び受信機を兼ね備える送受信機３３０を含む。場合によっては、送受信機３３０はネットワーク権限２００からローカルキー材料を受信するためにも使用される。送受信機３３０を介して、図３では第２のネットワークデバイス３２０である他のデバイスの識別番号が受信される。

【０１５１】

ネットワークデバイス３１０はローカルキー材料取得部３４４を備える。ローカルキー材料取得部３４４は、ローカルキー材料を記憶するためのローカルメモリ、例えばフラッシュメモリ等の不揮発性メモリとして実装され得る。また、ローカルキー材料取得部３４４は、例えば送受信機３３０を介して生成部２００からローカルキー材料を取得するよう構成されてもよい。ローカルキー材料取得部３４４は、多項式操作デバイスに必要なパラメータを提供するよう構成される。

【０１５２】

ネットワークデバイス３１０は多項式操作デバイス３４２を含む。多項式操作デバイス３４２は２つのフェーズで実行を行う。

【０１５３】

代入フェーズにおいて、第２のネットワークデバイスの識別番号がローカルキー材料内の各一変数多項式に代入される（５３０）。代入の結果は、当該一変数多項式に対応する公開モジュラスを法とする演算によりリダクションされる。次の加算フェーズにおいて、リダクションモジュロ公開モジュラスの結果が足し合わされ、モジュロ鍵モジュラスによってリダクションされる（５４０）。特定のN及び秘密モジュラスの組み合わせにおいては、結果を鍵モジュラスを法としたモジュロによってリダクションする前に２のべき乗による除算が要求されることに留意されたい。

【０１５４】

ネットワークデバイス３１０は、鍵モジュラスを法としたリダクションモジュロの結果から共有鍵を導出するための鍵導出デバイス３４６を含む。例えば、鍵導出デバイス３４６は１つ以上のLSBを除去し得る。また、鍵導出デバイス３４６は鍵導出関数を適用し得る。更なる処理を行うことなく、第２のリダクションの結果を使用することも可能である。

【０１５５】

ネットワークデバイス３１０は、オプションの鍵等化部（イコライザー）３４８を含む。第１のネットワークデバイスで導出された共有鍵と第２のネットワークで（第１のネットワークデバイスの識別番号に基づいて）導出された鍵が等しくない場合があることに留意されたい。これが望ましくないと考えられる場合、続いて鍵等化プロトコルが実行され得る。

【０１５６】

ネットワークデバイス３１０は、共有鍵を暗号アプリケーションに使用するよう構成された暗号要素３５０を含む。例えば、暗号要素３５０は、第１のネットワークデバイスのメッセージ、例えばステータスメッセージを第２のネットワークデバイスに送信する前に、共有鍵を用いてメッセージを暗号化又は認証し得る。例えば、暗号要素３５０は、第２のネットワークデバイスから受信されたメッセージを解読又はその真正性を検証し得る。

【０１５７】

典型的には、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２００、及び共有鍵を決定するよう構成される第１のネットワークデバイス３１０は、それぞれ、各デバイスに記憶される適切なソフトウェアを実行するマイクロプロセッサ（図示無し）を含み、例えば、ソフトウェアはダウンロードされて対応するメモリ、例えばRAM（図示無し）内に記憶されてもよい。

【０１５８】
a=1の場合、特により高い値のｍ 例えば1より大きい、2以上、又は4以上と組み合わせられる場合、興味深い実施形態が得られる。要求される多項式操作は単一の乗算及びリダクションに減少し、特に単純な実施形態を提供する。しかし、この単純なケースにおいてもオリジナルの二変数多項式を復元するのは簡単ではなく、mの値に比例して困難（複雑）になる。a=1についてさえ実行可能な攻撃は知られていないが、線形構造が将来の解析の出発点となり得るので、この理由のため、a>1に制約することが望まれることも考えられる。
【０１５９】
図４は、ローカルキー材料の生成方法４００を示す概略的なフローチャートである。方法４００はＴＴＰによって用いられ得る。ステップ４１０において、必要なパラメータが取得される。特に、複数の、少なくとも２つのパラメータセットが取得される。各パラメータセットは公開モジュラス及び少なくとも１つの秘密モジュラス、並びに少なくとも１つの二変数多項式を含む。ステップ４２０において、例えば遠隔通信ネットワークを介してネットワークデバイスの識別番号が取得される。識別番号は電子メッセージにより受信されてもよい。
【０１６０】
ステップ４３０はパラメータセットごとに一度ずつ繰り返される。取得された識別番号が二変数多項式に代入され、秘密モジュラスを法とする演算によりリダクションされる。より多くの、例えば２つの二変数多項式が存在してもよい。その場合、それぞれに代入され、結果が整数演算により加算される。ステップ４４０において、例えば難読化多項式を加えることによって結果が難読化される。単純な一実装形態では、難読化は単に単一の係数であり得る。ステップ４４０はオプションである。このようにすることで、又は本明細書に記載されるように、ローカルキー材料の一部を形成する一変数多項式と公開モジュラスの組み合わせが得られる。ステップ４５０において、パラメータセットが残っているか否かが判断され、残っている場合、次のパラメータセットに関してステップ４３０及び４４０が繰り返される。ステップ４５０において、難読化された一変数多項式を含むローカルキー材料がネットワークデバイスに保存される。
【０１６１】
図５は、共有鍵の生成方法５００を示す概略的なフローチャートである。方法５００はネットワークデバイスによって実行され得る。
【０１６２】
ステップ５１０において、例えば電子メッセージを受信することにより、他のネットワークデバイスの外部識別番号が取得される。ステップ５２０において、他のネットワークデバイスにローカル識別番号が送信される。ステップ５１０及び５２０の後、ローカルネットワークデバイス及び外部ネットワークデバイスは互いの識別番号を有する。各自のローカルキー材料を使用して、両者は共通の共有鍵の導出に進む。
【０１６３】
ローカルネットワークデバイスは、自身のローカルキー材料内の一変数多項式について代入ステップ５３０を繰り返す。ステップ５３０において、難読化された一変数多項式モジュロ対応する公開モジュラスに外部識別番号が代入される。ステップ５３５において、一変数多項式が残っているか否かが判断され、残っている場合、ローカルキー材料の次の一変数多項式についてステップ５３０が繰り返される。ステップ５４０において、リダクションモジュロ公開モジュラスの結果が足し合わされ、モジュロ鍵モジュラスによってリダクションされる。
【０１６４】
ステップ５５０の結果は、共有鍵取得の出発点である。ステップ５５０において、例えば鍵導出アルゴリズムを適用することにより、共有鍵が導出される。ステップ５６０において、他方のネットワークデバイスに鍵確認メッセージが送られ、ステップ５７０において、鍵が確認されたか否かが決定される。ステップ５７０で鍵が確認されない場合、方法

はステップ５５０に進んで新たな鍵を導出する。例えば、ステップ５５０は鍵が確認されない度にもう１つLSBを除去し得る。鍵が確認された場合、鍵はオプションの暗号アプリケーションにおいて使用されてもよいし、又は後の使用のためにローカルに保存されてもよい。

【０１６５】

ステップ５５０、５６０、及び５７０は、合わせて、鍵等化プロトコルを形成する。例えば、ステップ５６０において、ノンス、及びステップ５５０で導出された共有鍵によるノンスの暗号化が第２のデバイスに送信され得る。ステップ５６０において、第２のデバイスからメッセージが受信される。受信されたメッセージは、単純に受信された鍵確認メッセージが鍵が異なることを示した旨を表し得る。また、受信されるメッセージは鍵確認メッセージを含んでもよい。後者の場合、第１のネットワークデバイスは鍵確認メッセージを検証し、鍵が等しいか否かを確認する。鍵が等しくない場合、例えばLSBを消去することにより新たな鍵が導出される。

【０１６６】

図６は、２つのネットワークデバイスA及びBによる共有鍵の生成中の両デバイス間の可能なメッセージシーケンスを概略的な形式で示す。時間は下方向に進む。ステップ６１０において、ネットワークデバイスAは自身の識別番号をデバイスBに送信する。ステップ６２０において、デバイスBは自身の識別番号、並びに、識別番号A及び自身のローカルキー材料に基づいて導出した共有鍵（ K1）についての鍵確認メッセージを送信する。ステップ６３０において、デバイスAは両者が同じ鍵を生成しなかったことを発見した。デバイスAは１つのLSBを消去し（ 例えば、整数割る２ ）、鍵K2を得た。ステップ６３０において、デバイスAは新たな鍵確認メッセージを送信する。このようにして、A及びBは、ステップ６５０で同じ鍵にたどり着くまで鍵確認メッセージ６４０を交換する。ステップ６５０において、デバイスAは鍵確認メッセージをデバイスBに送信する。デバイスBは、両者が同じ鍵にたどり着いたことを検証できた。ステップ６６０において、デバイスBはその確認を送信し、これは認証メッセージ又は鍵確認メッセージ等であり得る。ステップ６７０において、デバイスAは同じになった共有鍵を用いて（ 例えば、AESを用いて）暗号化された及び／又は（ 例えば、HMACを用いて）認証されたメッセージMIを送信する。

【０１６７】

本発明は、本発明を実行するよう適合されたコンピュータプログラム、特にキャリア上の又はキャリア内のコンピュータプログラムまで及ぶ。プログラムは、ソースコード、オブジェクトコード、部分的にコンパイルされた形式等のソースコード及びオブジェクトコードの中間コードの形式、又は本発明に係る方法の実装形態に適した任意の他の形式を取り得る。コンピュータプログラム製品に関する一実施形態は、上記方法のうちの少なくとも１つの方法の処理ステップのそれぞれに対応するコンピュータ実行可能な命令を含む。これらの命令はサブルーチンに細分化されてもよいし、更に／又は静的に又は動的にリンクされ得る１つ以上のファイル内に保存されてもよい。コンピュータプログラム製品に関する他の実施形態は、上記システム及び／又は製品のうちの少なくとも１つの手段のそれぞれに対応するコンピュータ実行可能な命令を含む。

【０１６８】

上記実施形態は本発明を限定ではなく説明するものであり、当業者は多数の他の実施形態を設計できることに留意されたい。

【０１６９】

請求項において、括弧内の如何なる参照符号も請求項を限定すると解されるべきではない。動詞「 備える（ 又は含む若しくは有する等）」及びその活用形は請求項内に記載されている以外の要素又はステップの存在を除外しない。要素は複数を除外しない。本発明は、複数の異なる要素を備えるハードウェアによって、及び、適切にプログラミングされたコンピュータによって実施され得る。複数の手段を列挙する装置クレームにおいて、手段のいくつかは同一のアイテム又はハードウェアによって具現化されてもよい。単にいくつかの手段が互いに異なる独立請求項に記載されているからといって、これらの手段の組み

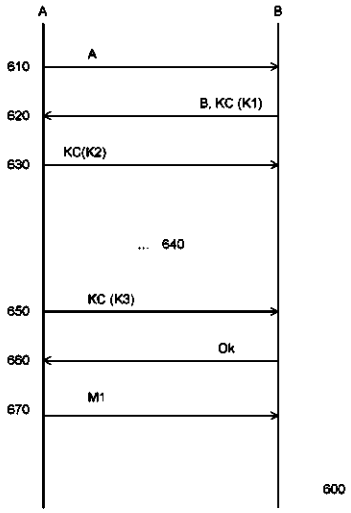
合わせを好適に使用することができないとは限らない。

【符号の説明】

【０１７０】

図１乃至図３の参照番号のリスト

１００　ルートキー材料取得部
１１０　公開モジュラスマネージャー
１１２　多項式次数要素
１１４　鍵長要素
１１６　多項式数要素
１２２　秘密モジュラスマネージャー
１２４　対称二変数多項式マネージャー
１３０、１４０　二変数多項式
１８０　ルートキー材料
２００　ローカルキー材料生成部
２１０　ルートキー材料要素
２２０　秘密材料要素
２４０　多項式操作デバイス
２５０　ネットワークデバイスマネージャー
２５２、２６２、２７２　一変数多項式
２６０　難読化数マネージャー
３００　通信ネットワーク
３１０　第１のネットワークデバイス
３２０　第２のネットワークデバイス
３３０　トランシーバ
３４２　多項式操作デバイス
３４４　ローカルキー材料取得部
３４６　鍵導出デバイス
３４８　鍵イコライザー
３５０　暗号要素



【 図 1 】

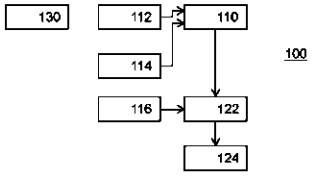


Figure 1

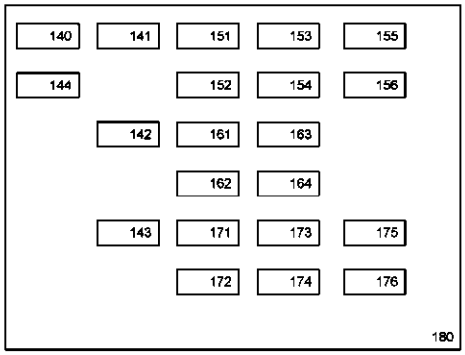


Figure 1'

【 図 2 】

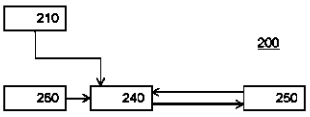


Figure 2

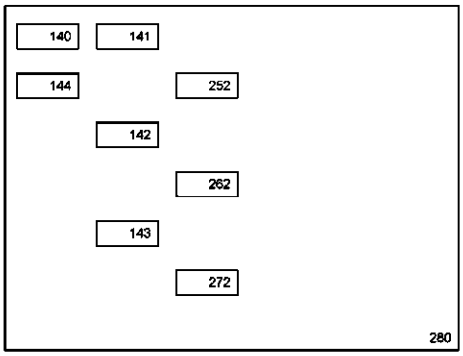


Figure 2'

【 図 3 】

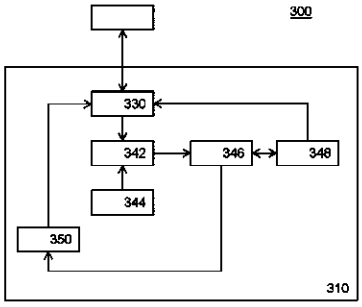
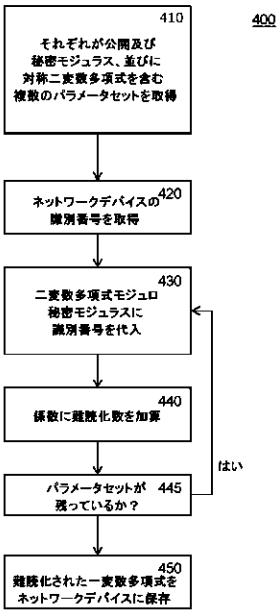
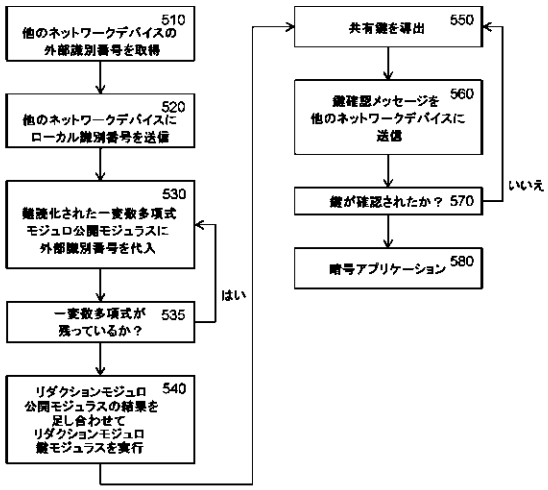


Figure 3

【 図４ 】


400
410
それぞれが公開及び
秘密モジュラス、並びに
対称二変数多項式を含む
複数のパラメータセットを取得
420
ネットワークデバイスの
識別番号を取得
430
二変数多項式モジュロ
秘密モジュラスに
識別番号を代入
440
係数に難読化数を加算
445
パラメータセットが
残っているか？
はい
450
難読化された一変数多項式を
ネットワークデバイスに保存

【 図５ 】


510
他のネットワークデバイスの
外部識別番号を取得
520
他のネットワークデバイスに
ローカル識別番号を送信
530
難読化された一変数多項式
モジュロ公開モジュラスに
外部識別番号を代入
535
一変数多項式が
残っているか？
はい
540
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
鍵モジュラスを実行
550
共有鍵を導出
560
鍵確認メッセージを
他のネットワークデバイスに
送信
570
鍵が確認されたか？
いいえ
580
暗号アプリケーション

フロントページの続き

(72)発明者　ゴメス　ドミンゴ
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　５
(72)発明者　ガルシア　モーション　オスカー
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　５
(72)発明者　トルフィツェン　ルドヴィクス　マリヌス　ジェラルダス　マリア
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　５
(72)発明者　グティエレス　ハイメ
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　５

審査官　青木　重徳

(56)参考文献　特許第５２７６５８４（ＪＰ，Ｂ２）
特許第５７５５３９１（ＪＰ，Ｂ２）
特表２０１２－５０３３５６（ＪＰ，Ａ）
特表２０１２－５２１１３６（ＪＰ，Ａ）
特表２０１２－５０３３９９（ＪＰ，Ａ）
欧州特許出願公開第１７９８８８９（ＥＰ，Ａ１）
飯田　達朗　ほか，ワイヤレスセンサネットワークにおける自己治癒機能を有する鍵共有方式の検討，情報処理学会研究報告　平成２２年度▲６▼［ＤＶＤ－ＲＯＭ］，日本，一般社団法人情報処理学会，２０１１年　４月１５日，Vol.2011-CSEC-52，No.31，ｐｐ．１－８
Chanjun Yang, et al., Pairwise Key Establishment for Large-scale Sensor Networks: from Identifier-based to Location-based (Invited Paper), InfoScale '06 Proceedings of the 1st international conference on Scalable Information Systems, ACM, ２００６年　５月２９日, Article No. 27

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／０８
ＪＳＴＰＬｕｓ／ＪＭＥＤＰＬｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ　Ｘｐｌｏｒｅ
ＴＨＥ　ＡＣＭ　ＤＩＧＩＴＡＬ　ＬＩＢＲＡＲＹ