(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2015-521001
(P2015-521001A)
(43)公表日　平成27年7月23日(2015.7.23)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601C	5J104
G09C	1/00	(2006.01)	G09C	1/00	610Z	

審査請求 有　予備審査請求 有　（全 39 頁）

(21)出願番号	特願2015-513055 (P2015-513055)
(86)(22)出願日	平成25年3月28日 (2013.3.28)
(85)翻訳文提出日	平成26年11月21日 (2014.11.21)
(86)国際出願番号	PCT/EP2013/056730
(87)国際公開番号	WO2013/174554
(87)国際公開日	平成25年11月28日 (2013.11.28)
(31)優先権主張番号	61/649,464
(32)優先日	平成24年5月21日 (2012.5.21)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	12168710.7
(32)優先日	平成24年5月21日 (2012.5.21)
(33)優先権主張国	欧州特許庁 (EP)
(31)優先権主張番号	61/658,475
(32)優先日	平成24年6月12日 (2012.6.12)
(33)優先権主張国	米国 (US)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エヌヴェ
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
(74)代理人　110001690
特許業務法人M&Ｓパートナーズ
(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　ビルディング　５

最終頁に続く

(54)【発明の名称】鍵共有デバイス、及び鍵共有デバイスを構成するためのシステム

(57)【要約】
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が提供される。構成方法は秘密モジュラスp_1及び公開モジュラスN、並びに整数の係数を有する二変数多項式f_1を使用し、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。二変数多項式に識別番号を代入し、代入の結果に秘密モジュラスを法としたリダクションモジュロを行って一変数多項式を得ることによって、ネットワークデバイスのローカルキー材料が生成される。一変数多項式の係数に１つ以上の難読化数を加えて４４０難読化された一変数多項式を得ることによってセキュリティが高められ得る。使用フェーズでは、ネットワークデバイスが他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５３０し、公開モジュラスを法としたリダクションモジュロを行い鍵モジュラスを法としたリダクションモジュロを行うことによって共有暗号鍵を決定する。

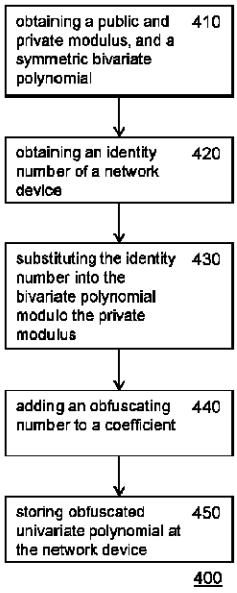

Figure 4

【特許請求の範囲】
【請求項１】
鍵共有のためにネットワークデバイスを構成する方法であって、前記方法は、
秘密モジュラス、公開モジュラス、及び整数の係数を有する二変数多項式を電子形式で取得する取得ステップであって、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、取得ステップと、
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生成ステップであって、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、前記代入の結果に前記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ことにより前記二変数多項式から一変数多項式を決定するステップとを含む、生成ステップと、
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保存ステップと、
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生成ステップは、難読化数を生成するステップと、多項式操作デバイスを使用して、前記難読化数を前記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】
前記二変数多項式は対称多項式である、請求項１又は２に記載の方法。
【請求項４】
前記公開モジュラスのバイナリ表現の最下位の前記鍵長ビットは、前記秘密モジュラスの最下位の前記鍵長ビットと同じである、請求項１乃至３のいずれか一項に記載の方法。
【請求項５】
電子乱数生成部を使用して前記秘密モジュラスを生成するステップと、
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って、電子乱数生成部を使用して前記二変数多項式を生成するステップと
を含む、請求項１乃至４のいずれか一項に記載の方法。
【請求項６】
前記公開モジュラスは$2^{(a+2)b-1} \leq N$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５のいずれか一項に記載の方法。
【請求項７】
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と、係数秘密モジュラスを法としたモジュロを有する複数の二変数多項式とを取得するステップを含み、
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、それぞれの対称二変数多項式に前記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、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６のいずれか一項に記載の方法。
【請求項８】
前記難読化数は、

$$|\varepsilon_{A,i}| < 2^{(a+1-i)b}$$

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７のいずれか一項に記載の方法。
【請求項９】

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であって、前記方法は、
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、任意で難読化されていてもよい一変数多項式を含む、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、
前記第２のネットワークデバイスの前記識別番号を前記任意で難読化されていてもよい一変数多項式に代入するステップと、
前記代入の結果に前記公開モジュラスを法としたリダクションモジュロを行い、鍵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、
前記鍵モジュラスを法とした前記リダクションモジュロ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１０】
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、前記鍵モジュラスを法とした前記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を更に含む、請求項９に記載の方法。
【請求項１１】
前記代入の結果前記公開モジュラスを法としたモジュロを、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を更に含み、前記０ビット列除数は１より大きい、請求項９又は１０に記載の方法。
【請求項１２】
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、前記システムは、
秘密モジュラス、公開モジュラス、及び整数の係数を有する対称二変数多項式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が、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、前記代入の結果に前記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ことによって前記二変数多項式から一変数多項式を決定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１３】
暗号鍵である共有鍵を決定するための第１のネットワークデバイスであって、前記第１のネットワークデバイスは、
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任意で難読化されていてもよい一変数多項式を含む、ローカルキー材料取得部と、
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ための受信機と、
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任意で難読化されていてもよい一変数多項式に代入し、前記代入の結果に前記公開モジュラスを法としたリダクションモジュロを行い鍵モジュラスを法としたリダクションモジュロを行うための多項式操作デバイスと、

前記鍵モジュラスを法とした前記リダクションモジュロ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、第１のネットワークデバイス。
【請求項１４】
コンピュータ上で実行されたとき、請求項１乃至１１のいずれか一項に記載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コンピュータプログラム。
【請求項１５】
コンピュータ読み取り可能媒体に取り込まれた請求項１４に記載のコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、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、当該方法は、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って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のネットワークが暗号鍵である共有鍵を決定するための方法に関連し、当該方法は、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、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】
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。
【０００５】
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。
【０００６】
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。
【０００７】
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起こる（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。

【０００８】
Song Guo、Victor Leung、及びZhuzhong Qianによる“A Permutation-Based Multi-Polynomial Scheme for Pairwise Key Establishment in Sensor Networks”, IEEE International Conference on Communications, 2010が参照される。この文献は、無線センサネットワークにおけるペアワイズ鍵確立のための置換（permutation）ベースの複数多項式スキームを提唱する。Songにより提唱されるスキームは、Blundoとは異なり、各ノードに単一の対称多項式を割り当てるのではなく、置換のグループを割り当てる。
【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。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、及び整数の係数を有する二変数多項式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、代入の結果に秘密モジュラスを法としたリダクションモジュロ（秘密モジュラスを法とする計算）を行うことにより二変数多項式から一変数多項式を決定するステップとを含む、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。一実施形態では、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は、例えば電子乱数生成部を使用することによって難読化数を生成するステップと、多項式操作デバイスを使用して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ステップとを含み、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。２つ以上の係数が難読化されてもよく、好ましくは、異なる係数には異なる難読化がされる。一実施形態では、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は、例えば電子乱数生成部を使用して複数の難読化数を生成するステップと、多項式操作デバイスを使用して、複数の難読化数の各難読化数を一変数多項式の対応する係数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む。一実施形態では、一変数多項式の各係数に難読化数が加えられ得る。
【００１１】
二変数多項式は対称でもよいし、非対称でもよい。二変数多項式又は複数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有鍵を導出し得る。興味深いことに、ルートキー材料として、複数の二変数多項式の中に１つ以上の非対称二変数多項式を用いることにより、２つのデバイスグループの作成に適合することが可能になる。例えば、同じグループに属する２つのデバイスは共通鍵を生成できないが、異なるグループ内の２つのデバイスは可能である。
【００１２】
難読化を加えることは任意の（オプションの）ステップである。ローカルキー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ので、難読化がなくとも攻撃に対する保護は依然として得られ、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が妨害される。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いことを意味する。一方、秘密モジュラスと公開モジュラスとが複数の連続ビットで重複するため、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。一変数多項式の係数に１つ以上の難読化数を加えて難読化された一変数多項式を得ることにより、セキュリティが高められる。しかし、難読化数を加

えるステップは任意であり、省略されてもよい。難読化を加えるか否かは、正しく共有鍵を導出する可能性と付加的なセキュリティとの間のトレードオフである。

【００１３】

公開モジュラスはネットワークデバイス内で使用されるためのものである。鍵共有のためにネットワークデバイスを構成する方法は、ネットワークデバイスが公開モジュラスを利用できるようにすること、例えば、公開モジュラスをローカルキー材料と共に記憶することを含み得る。

【００１４】

第１のネットワークデバイスの共有鍵（暗号鍵）を決定する方法は、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、任意で難読化されていてもよい一変数多項式を含む、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、第２のネットワークデバイスの識別番号を任意で難読化されていてもよい一変数多項式に代入するステップと、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を行い鍵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、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を含む。一実施形態では、方法は例えば、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、鍵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を含む。

【００１５】

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。

【００１６】

ローカルキー材料が対称多項式から得られた場合、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ができる。ローカルキー材料に難読化数が加えられた場合、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。

【００１７】

難読化が使用されなかったとしても、公開モジュラスと（１つ又は複数の）秘密モジュラスとは異なるので、攻撃は依然として困難である。難読化されない場合でも、公開モジュラスを法としたリダクションモジュロは同じ共有鍵を導出する可能性を高める。

【００１８】

一実施形態では、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。

【００１９】

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。

【００２０】

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。

【００２１】

一実施形態では、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。

【００２２】

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。

【００２３】

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。

【００２４】

複数の秘密モジュラス中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。

【００２５】

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。

【００２６】

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得り、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。

【００２７】

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。

【００２８】

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。

【００２９】

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。

【００３０】

一実施形態では、公開モジュラスNは$2^{(a+2)b-1} \leq N \leq 2^{(a+2)b}-1$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。

【００３１】

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。

【００３２】

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。

【００３３】

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。

【００３４】

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。

【００３５】

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、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。

【００３６】

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。

【００３７】

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。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。

【００３８】

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ニ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。

【００３９】

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、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、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。

【００４０】

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。

【００４１】

次数aの変数x及びyの対称二変数多項式は、形式x^iy^jの単項式しか有さない（$i \leq a$、$j \leq a$）。更に、x^iy^jに対応する係数は、x^jy^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^jy^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。

【００４２】

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。

【００４３】

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。

【００４４】

難読化がない場合でも、第１のネットワークデバイスによって導出される共有鍵が全て

のビットにおいて第２のネットワークデバイスによって導出される共有鍵と同じではない可能性があることに留意されたい。ただし、その可能性は難読化を有するケースより低い。

【００４５】

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。

【００４６】

また、難読化数の選択も制御され得り、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、$|\varepsilon_{A,i}|<2^{(a+1-i)b}$が要求され得り、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。

【００４７】

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。

【００４８】

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。

【００４９】

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。

【００５０】

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気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気的に送信して、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。

【００５１】

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。

【００５２】

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。

【００５３】

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。

【００５４】

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。

【００５５】

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、デバイス上に記憶されるローカルキー材料を生成する整数に加えられる。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。例えば、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おいて多変数多項式が使用され得り、方法は、秘密モジュラス（p_1）、公開モジュラス（N）、及び整数の係数を有する多変数多項式（f_1）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（b）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（A）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、多変数多項式に識別番号を代入し、代入の結果に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ことにより多変数多項式から多項式を決定するステップとを含む、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。多項式操作デバイスによって得られる多項式の変数は１少ない。複数の変数が全ての変数について対称である場合、鍵共有にとって好都合である。対応する、第１のネットワークデバイスが共有鍵（暗号鍵）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、任意で難読化されていてもよい多項式を含む、ステップと、複数の他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、複数の他のネットワークデバイスの識別番号を任意で難読化されていてもよい多項式に代入するステップと、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を行い鍵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、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を含む。１つの識別番号を除く全ての他の識別番号の代入後、方法は一変数多項式が使用される状況になることに留意されたい。

【００５６】

一実施形態では、第１のネットワークデバイスはそのデバイスの識別番号に関連付けら

れた複数の（n）ローカルキー材料を受信する。この第１のデバイスと第２のデバイスとの間で生成される鍵は、第２のデバイスの識別番号を用いて複数の（n）第１のデバイスのローカルキー材料のそれぞれを評価することによって得られる複数の（n）鍵の組み合わせ（例えば、連結）として得られる。これは方法の並列使用を可能にする。

【００５７】

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)!=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。

【００５８】

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。

【００５９】

一実施形態では、対称多項式は$\langle ax^iy^i\rangle_{p_j}$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。

【００６０】

鍵共有のためにネットワークデバイスを構成する方法の一実施形態では、方法は、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ような鍵長（b）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（p_i）、及び整数の係数を有する複数の二変数多項式（f_i）を電子形式で取得するステップと、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（A）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、識別番号を複数の二変数多項式のそれぞれに代入し、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い、複数のリダクションの複数の結果を加算することによって複数の二変数多項式から一変数多項式を決定するステップとを含む、ステップと、難読化数を生成して、多項式操作デバイスによって一変数多項式の係数に加えることによって難読化された一変数多項式を得るステップとを含み、生成されたローカルキー材料は難読された一変数多項式を含み、ネットワークデバイスに電子的に保存される。複数の二変数多項式(f_i)の二変数多項式は、対応する秘密モジュラス（p_i）を法とした係数モジュロを有するとして表され得る。

【００６１】

より一般的には、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。

【００６２】

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、秘密モジュラスより大きい又は小さくてもよい公開モジュラス、及び整数の係数を有する対称二変数多項式を電子形式で取得するための鍵材料取得部であって、公開モジュラスマイナス秘密モジュラスのバイナリ表現の鍵長ビット（場合によっては、鍵長のLSB）は全て０である、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、二変数多項式に識別番号を代入し、代入の結果に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ことによって二変数多項式から一変数多項式を決定するための多

項式操作デバイスとを含む、生成部とを含む。

【００６３】

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。

【００６４】

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難読化された一変数多項式を含む、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機と、第２のネットワークデバイスの識別番号を任意で難読化された一変数多項式に代入し、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を行い鍵モジュラスを法としたリダクションモジュロ（公開モジュラスと鍵モジュラスは互いに素）を行うための多項式操作デバイスと、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とを含む。

【００６５】

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。

【００６６】

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。

【００６７】

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。

【００６８】

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。

【００６９】

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ナンス等でもよく、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。

【００７０】

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。

【００７１】

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。

【００７２】

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。

【００７３】

完全さのために、発明の名称が“A method for secure communication in a network, a communication device, a network and a computer program therefor”である国際出願WO2010032161について言及する。この出願は、通信ネットワークにおける安全な通信のための方法に関する。

【００７４】

本願と上記出願との間には複数の違いが存在し、モジュラ演算の使用、特に異なる公開及び秘密モジュラスを有するモジュラ演算の組み合わせ、モジュラ演算の反復、例えば公開モジュラスを法としたリダクションモジュロ及びその後の鍵モジュラスを法としたリダクションモジュロ、難読化の使用、多項式全体の使用が含まれる。

【００７５】

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が提供される。構成方法は秘密モジュラスp_1及び公開モジュラスN、並びに整数の係数を有する二変数多項式f_1を使用し、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。二変数多項式に識別番号を代入し、代入の結果に秘密モジュラスを法としたリダクションモジュロを行って一変数多項式を得ることによって、ネットワークデバイスのローカルキー材料が生成される。一変数多項式の係数に１つ以上の難読化数を加えて４４０難読化された一変数多項式を得ることによってセキュリティが高められ得る。使用フェーズでは、ネットワークデバイスが他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５３０し、公開モジュラスを法としたリダクションモジュロを行い及び鍵モジュラスを法としたリダクションモジュロを行うことによって共有暗号鍵を決定する。

【図面の簡単な説明】

【００７６】

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。

【００７７】

【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。

【００７８】

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。

【符号の説明】

【００７９】
１００　ルートキー材料取得部
１１０　公開モジュラス要素
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
２００　ローカルキー材料生成部
２１０　公開材料要素
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
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
【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先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
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。
【００８４】
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」の値は拡張されたhidden number problem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。

【００８５】

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。複雑性の低いアプリケーション、例えば資源制約デバイスのためにはm=1を使用し得ることに留意されたい。

【００８６】

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。

【００８７】

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。

【００８８】

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。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。

【００８９】

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。

【００９０】

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。

【００９１】

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。二変数多項式の一部又は全てが非対称に生成されてもよいことに留意されたい。この場合、システムが２つのグループを有することになる。単純さのため、全ての選択多項式が対称であると仮定する。

【００９２】
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，...，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）。

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

【００９３】
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、割り当てられる多項式が整数に加えられるとき、多項式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。

【００９４】
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、$p_j=2^X+\gamma_j 2^{Yj}-1$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。

【００９５】
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、$p_j=\beta 2^X+\gamma_j 2^{Yj}+\zeta_j 2^{Zj}$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$\gamma_j 2^{Yj}$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。

【００９６】
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。

【００９７】
TTPはデバイスAのための鍵材料のセットを以下のようにして生成する。

$$KM^A(X) = \sum_{j=1}^{m} < f_j(x,A) >_{p_j} + 2^b \sum_{i=0}^{a} \epsilon_{A,i} X^i = \sum_i C_i^A x^i$$

【００９８】
ここで、$KM^A(X)$は識別番号Aのデバイスの鍵材料であり、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。$<\cdot\cdot\cdot>p_j$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$|\varepsilon_{A,i}|<2^{(a+1-i)b}$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

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

は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、

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

が小さい、例えば<2aである。難読化を加えるステップは任意であり省略され得るが、より高いセキュリティレベルを得るためには好ましいことに留意されたい。難読化が用いられると仮定する。
【００９９】
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

$$2^b \sum_{i=0}^{a} \epsilon_{A,i} X^i$$

の加算も普通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^A（i=0,...,a）を含む。鍵材料は上記のような多項式として示され得る。実際には、鍵材料は整数C_i^Aのリスト、例えば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。
【０１００】
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。
【０１０１】
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。

$$K_{AB} = << KM^{A}(x)|_{x=B} >_{N} >_{2^{b}} = \ll \sum_{i} C_{i}^{A} B^{i} >_{N} >_{2^{b}}$$

【０１０２】

つまり、Aは整数多項式として見られる自身の鍵材料を値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公開モジュラスNを法としたモジュロによってリダクションし、続いて鍵モジュラス2^{b}を法としたモジュロによってリダクションする。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ってBの共有鍵を生成できる。

【０１０３】

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。特にネットワークデバイス上に記憶される鍵材料の係数の最下位の（複数の）ビットに非線形効果が導入され、Nの式の２番目の項がY_{j}の場合、鍵は以下のようにして生成される。

$$K_{AB} = < \frac{< KM^{A}(x)|_{x=B} >_{N}}{2^{Y_{j}}} >_{2^{b}}$$

【０１０４】

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。整数p_{1}，p_{2}，...，p_{m}及び（オプションの）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得り、例えば様々な暗号アプリケーションのために使用し得り、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。

【０１０５】

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。

【０１０６】

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に状況を知らせるべく応答してもよい。

【０１０７】

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。

【０１０８】

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。

【０１０９】

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、γ_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。

【０１１０】

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。

【０１１１】

上記したように、差$Y_j-Z_j-\log_2(\zeta_j)$は$\alpha_j b$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割り当て多項式の係数の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、異なる環内の割り当て多項式の係数が整数に加えられることによって寄与の起源が隠される。

【０１１２】

鍵は

$$K_{AB}=<\frac{<KM^A(x)|_{x=B}>_N}{2^{Y_j}}>_{2^b}$$

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。

【０１１３】

鍵確認

A及びBの一方が鍵確認メッセージを他方の機関に送信することが望ましい場合がある。いわゆる鍵確認メッセージ（KC）は、鍵確認メッセージの受信者が自身が鍵確認メッセージの送信者と同じ鍵を計算したことを検証することを可能にする。特に両機関によって確立された鍵が異なり得ることが知られている鍵共有スキームでは、鍵確認メッセージが、両者が同じ鍵を確立したことの確認として、且つ、鍵が異なる場合、同じ共有鍵を決定するために使用され得る。例えば、一般的に、確立された鍵に基づくMAC、例えばSHA２若しくはSHA３に基づくHMAC、又はAESに基づくCMAC等が確認メッセージとなり得る。また、暗

号的に強力なハッシュ関数、例えば確立された鍵のハッシュが鍵確認メッセージとして使用されてもよい。ハッシュは鍵自体について計算されてもよい。MACはBによって知られているデータ又は鍵確認メッセージ内に含まれているデータ、例えばナンス等について計算されてもよい。

【０１１４】

しかし、一般的な暗号的に強力な鍵確認メッセージはいくらかの資源を要求し、上記原理に係る鍵共有アルゴリズムより多くの資源を要求する可能性がある。上記の鍵共有スキームは、汎用鍵確認スキームよりはるかに少ない計算資源を要求する単純な機能を可能にする。

【０１１５】

デバイスA及びBは鍵$K_A(B)$及び$K_B(A)$を計算する。上記数学的関係に従うことにより、設計パラメータに応じて、次式のような整数Δが存在することが示され得る。

$$K_A(B) \in \{ < K_B(A) + j >_{2^b} \mid -\Delta \leq j \leq \Delta \}$$

【０１１６】

上記と同様に、$<x>_m$はx-$<x>_m$がmの倍数であるような0からm-1の整数を表す。次のような関数を定義する：$h(x)= <x>_{2^r}$。ここで、rは$2^r \geq 2\Delta+1$であるような所定の整数である。一般的な実施形態と比較すると、デバイスが複雑であり得るハッシュ関数を計算する必要がないが、デメリットは、使用されている鍵に関する情報の一部が監視可能な通信チャネルを介して送信されることである。通常、計算された鍵確認メッセージは鍵に関する情報を全く又は無視できる量しか漏らさないことが好ましい。このデメリットは、A及びBの両方に関して同じである鍵が発見された後、確立された鍵を2^rによって割ることにより対処できる。より一般的な第２の実施形態では、$h(x)=<x>_v$であり、ここで、$v \geq 2\Delta+1$は、2^bがvの倍数、又は$<2^b>_v \geq 2\Delta+1$を満たす。いずれにせよAは鍵確認メッセージとして$h(K_A(B))$を使用し得る。

【０１１７】

鍵確認メッセージを送信する他に、両鍵を2のべき乗で割ることによって$K_A(B)$及び$K_B(A)$間の違いを減らしてもよい。$K_A(B)$及び$K_B(A)$がbビットの鍵である場合、bビットの生成鍵の1個のLSBを除去して、b-1MSBに対応する生成されるb-1ビット鍵を使用して安全な通信を実現してもよい。bが比較的大きく（例えば、100）、1も同様に大きい（例えば、50）場合、b-1MSBが等しくなる確率は非常に高く、すなわち約$1-(2\Delta/2(b-1))$である。このアプローチは如何なる情報の交換も必要とせず、オリジナルの生成鍵の1ビットを除去することにより得られる鍵を通信に使用できる。しかし、鍵サイズが（場合によっては相当に）低減されるので、非常に高い確率でネットワーク内の全てのデバイスが共通のb-1ビットの鍵を共有することを確認するという欠点がある。

【０１１８】

LSBの除去は鍵確認メッセージと組み合わせられ得ることに留意されたい。例えば、1ビットの除去後に鍵確認メッセージが計算され、他の機関に送信される。このアプローチは、たとえLSBの除去が共通鍵を確立するのに十分ではなかったとしても、かかる共通鍵を発見することを容易にするという利点を有する。

【０１１９】

機関A及びBによって確立される潜在的に異なる鍵の問題の他のアプローチは以下の通りである。任意の２つのデバイスが異なる鍵を導出し得る場合に計算すべき全ての情報を中央権限が事前に備える。例えば、中央権限は単一の識別子A及びAのために計算される鍵材料から開始し得る。デバイスがデバイスのプールに繰り返し追加される。システムに新たなデバイスB’が追加されるとき、TTPはB’の鍵材料を計算する。TTPは、B’とプール内に既に存在するデバイスとのそれぞれの組み合わせについて、同じ共通鍵にたどり着くか否かを検証する。例えば、TTPはデバイスが同じ鍵を直接発見することを検証し得る。また、TTPは、潜在的に異なる鍵を修復するための適切な鍵合意プロトコルに従事することによって、例えば、2のべき乗で割ることによって及び／又は１つ以上の鍵確認メッセー

ジを送信することによって、B’及び任意の他のデバイスが共通鍵にたどり着くことを検証してもよい。上記確率的アプローチを考慮すると、デバイスAの個数が比較的小さい場合、ランダムに選択されるB’が全てのAについて{A,B’}を有効とする可能性が非常に高い。

【０１２０】

B’がプール内に既に存在するデバイスの一部に関して共通鍵にたどり着かない場合、TTPは、異なるランダム選択をして、B’に新たな識別子を割り当てる又は新たな鍵材料を計算する。この条件の確認は相当なオーバーヘッドを課すが、比較的小さいネットワークでは可能である（例えば、～$O(10^4)$又は$O(10^5)$個のデバイス）。

【０１２１】

関連するアプローチはグループ分けされたデバイスにも適用できる。特に、ある設定では、例えばデバイスが静的でありグループとして（例えば、建物内に）配置されている場合、全てのデバイスが互いに通信する必要がないことがある。この場合、新たなデバイスB’が追加されるときにTTPによって実行される検証は、B’が追加されるグループに属するデバイスに対するチェックに限定される。例えば、TTPは、所与のグループ内の全デバイスが、鍵の1LSBが除去された場合にある鍵を生成するか否かを検証し得る。また、この方法は、第１のレベルでは全てのデバイスがメイングループに属し、第２のレベルではデバイスが複数のグループに分割され、第２のレベルのグループ内のデバイスが更に複数のサブグループに分割されるようなより高度な階層スキームの設計も許容することに留意されたい。かかる階層構造では、TTPは、レベルwの所与のグループ内の全デバイスが1_wビットの除去後に共通鍵を生成するか否かを検証してもよい。かかるシステムでは、低いレベルにおけるグループはより少ないビット数の除去を要求する一方、高いレベルにおけるグループは、共通鍵の生成を確実にするために、より多くのビットの除去を要求し得る。

【０１２２】

TTPは新たなデバイスが追加される度にこれらのチェックを実行してもよいが、識別子の各ペアが有効な共通鍵を与えるようなデバイス識別子及び鍵材料のプールを積極的に作成してもよい。

【０１２３】

例えば、TTPは有効なデバイスのペア{A,B}に限定してもよく、ここでペアは以下の場合に有効である。

$$\left\lfloor \frac{K_B(A)}{2^l} \right\rfloor = \left\lfloor \frac{K_A(B)}{2^l} \right\rfloor$$

ここで、lは$K_A(B)$及び$K_B(A)$の1LSBに対応するlビットを指す。この条件は、概して、実際に使用される鍵が等しいことを検証する一方法を示す。別の条件は、全てのAについて$K_A(B)$及び$K_B(A)$の1LSBが［Δ，$2^l-1-\Delta$］内の数字に対応する場合にのみ新たなBが許可されるというものである。

【０１２４】

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、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。

【０１２５】

ルートキー生成部１００は、それぞれが多項式次数、鍵長、及び多項式の数、すなわちa、b、及びmを提供（供給）するよう構成される多項式次数要素１１２、鍵長要素１１４、及び複数の多項式要素１１６を備える。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。

【０１２６】

ルートキー生成部１００は、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。

【０１２７】

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，...，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。

【０１２８】

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，...，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得り、ランダムで選択され得る。

【０１２９】

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。

【０１３０】

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。

【０１３１】

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に公開パラメータa、Nを提供するための公開材料要素２１０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に秘密パラメータp_i、f_i、及びmを提供するための秘密材料要素２２０を含む。要素２１０及び２２０は鍵材料生成部１００の対応する要素によって実現され得り、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。

【０１３２】

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。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。

【０１３３】

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、又はナ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。

【０１３４】

多項式操作デバイス２４０は、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）。

【０１３５】

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。

【０１３６】

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。

【０１３７】

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。

【０１３８】

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。

【０１３９】

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の識別番号を難読化された一変数多項式に代入し、その結果に２つのリダクションを実行する、すなわち、代入の結果をまず公開モジュラスを法としたモジュロによって、次に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よう構成される多項式操作デバイス３４２を含む。たとえ複数の秘密モジュラスが使用されたとしても、単一の公開モジュラスのみが必要であることに留意されたい。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。

【０１４０】

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。

【０１４１】

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。

【０１４２】

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。

【０１４３】

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。

【０１４４】

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。

【０１４５】

図４は、ローカルキー材料４００の生成方法を示す概略的なフローチャートである。方法は、公開及び秘密モジュラス、並びに対称二変数多項式を取得するステップ４１０と、ネットワークデバイスの識別番号を取得するステップ４２０と、識別番号を、秘密モジュラスを法とした二変数多項式モジュロに代入するステップ４３０と、係数に難読化数を加えるステップ４４０と、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するステップ４５０とを含む。

【０１４６】

図５は、共有鍵５００の生成方法を示す概略的なフローチャートである。方法は、他のネットワークデバイスの外部識別番号を取得するステップ５１０と、他のネットワークデバイスにローカル識別番号を送信するステップ５２０と、外部識別番号を難読化された公開モジュラスを法とした一変数多項式モジュロに代入するステップ５３０と、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ステップ５４０と、共有鍵を導出するステップ５５０と、他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ステップ５６０と、鍵が確認されたか否かを決定するステップ５７０と、暗号アプリケーション５８０とを含む。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更に１つのLSBを除去し得る。

【０１４７】

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、ナンス、及びステップ５５０で導出された共有鍵によるナンスの暗号化が第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。

【０１４８】
当業者にとって明らかなように、当該方法は多様に実行可能である。例えば、ステップの順番は変更され得り、一部のステップは並列に実行され得る。また、ステップ間に他の方法ステップが挿入されてもよい。挿入されるステップは本明細書が開示するような方法の改良に相当してもよいし、方法とは無関係でもよい。例えば、ステップ４１０及び４２０、又は５１０及び５２０は、少なくとも部分的に並列に実行され得る。また、所与のステップが完全に終了する前に次のステップが開始されてもよい。
【０１４９】
本発明に係る方法は、プロセッサシステムに方法４００又は５００を実行させるための命令を含むソフトウェアを用いて実行され得る。ソフトウェアは、システムの特定のサブエンティティによって実行されるステップのみを含んでもよい。ソフトウェアはハードディスク、フロッピー（登録商標）、メモリ等の適切な記憶媒体内に記憶され得る。ソフトウェアは有線若しくは無線による信号として、又はインターネット等のデータネットワークを用いて送信され得る。ソフトウェアはダウンロード及び／又はサーバ上での遠隔使用により利用可能でもよい。
【０１５０】
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M1を送信する。
【０１５１】
以下のアルゴリズムはこのアプローチ、すなわち、デバイスA及びBによって実行される相互鍵合意及びセッション鍵導出のためのプロトコルの可能な実装形態を与える。

```
Set l=L
Set continue=TRUE
Set Length = b-l
Generate a b-bit key K
While(continue AND (Length>MINIMUM_LENGTH)){
      K = K>>l
      Perform Mutual authentication handshake with B based on K
      If handshake successful, then{
            continue=FALSE
      }}else{
           Length = b-l
}
```

【０１５２】
プロトコルは、本明細書に開示されるような鍵共有アルゴリズムを用いて生成されたビット列の複数のビットを除去し、認証ハンドシェイク、例えばチャレンジレスポンスを実行する。認証ハンドシェイクは鍵確認メッセージを含み得る。成功しない場合、更にいく

つかのビットが除去され、ハンドシェイクが成功するまで又は鍵が短くなり過ぎるまで繰り返される。プロトコルは多様に変更され得り、例えば、プロトコルの実行を監視している傍受者がAとBとの間で共有される共通鍵の長さについて如何なる情報も得られないよう、反復に応じて可変のビット数を除去することによって、又は常に一定数のステップを要求することによって変更され得る。このアプローチは、共有鍵が可能な限り長いことを保証するという利点を有するが、共通鍵に関する合意のために複数の交換を要するという潜在的なデメリットを有する。一方、ほとんどのアプリケーションではこれは大きな問題とならない。ほとんどのデバイスペアにおいて鍵は等しくなる又は数ビットしか違わず、比較的多数の異なるLSBに至るのは少数のデバイスペアのみだからである。これは生成される鍵の特性による。

【０１５３】

両デバイスが同じ鍵にたどり着くための他の方法も存在する。再び、デバイスA及びBが鍵$K_A(B)$及び$K_B(A)$を計算すると仮定する。以下のプロトコルは、設計パラメータに依存する次のような整数Δが存在するあらゆる鍵共有スキームに適用される。

$$K_A(B) \in \{ < K_B(A) + j >_{2^b} \mid -\Delta \leq j \leq \Delta \}$$

【０１５４】

例えば、本明細書に開示される鍵共有スキームはこの特性を有する。生成される鍵はbビットの整数として表される。したがって、鍵はセット{0，1，2，...，2^b-1}からの要素であると考えられる。例えば、Δ＝２且つ$K_B(A)=1$の場合、$K_A(B)$は{1，2，3，0，2^b-1}に含まれる（

$$< 1-2 >_{2^b} = 2^b - 1$$

であることに留意されたい）。適切に選択されたシステム設計パラメータに対して、Δは比較的小さい。共通鍵生成の失敗から立ち直ることができるので、本発明は常に同じ鍵が生成されることを保証する。

【０１５５】

当該方法によれば、デバイスAは関数値$h(K_A(B))$をデバイスBに送信する。ここで、hは適切なハッシュ関数、例えば暗号ハッシュ関数である。デバイスBは

$$\{ < K_B(A) + j >_{2^b} \mid -\Delta \leq j \leq \Delta \}$$

内の全てのiについてh(i)を計算し、h(i)が受信された$h(K_A(B))$の値と一致する整数iを将来の通信に使用する。Δが大き過ぎる場合、デバイスA及びBはまず鍵を２のべき乗で割ることによってΔのサイズを減少し得る。

【０１５６】

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。

【０１５７】

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。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。

【図１】

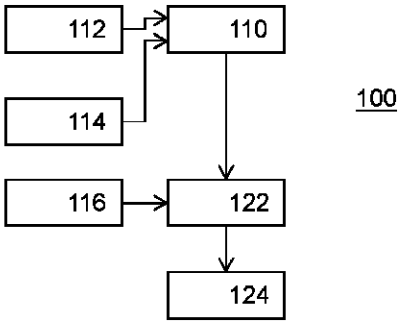

Figure 1

【図２】

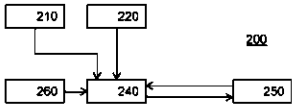

Figure 2

【図３】

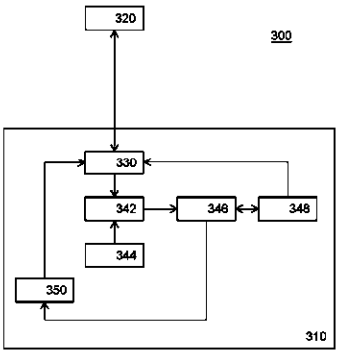

Figure 3

【図６】

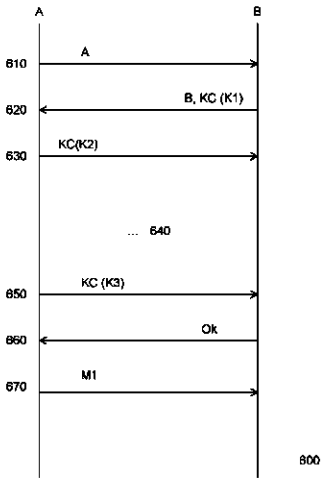

Figure 6

【図４】

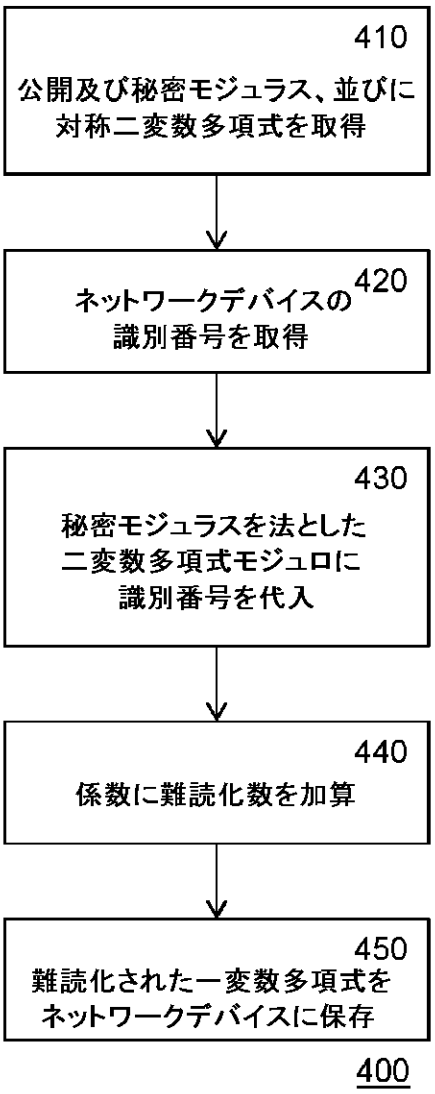
410
公開及び秘密モジュラス、並びに
対称二変数多項式を取得
420
ネットワークデバイスの
識別番号を取得
430
秘密モジュラスを法とした
二変数多項式モジュロに
識別番号を代入
440
係数に難読化数を加算
450
難読化された一変数多項式を
ネットワークデバイスに保存
400

図４

【図５】

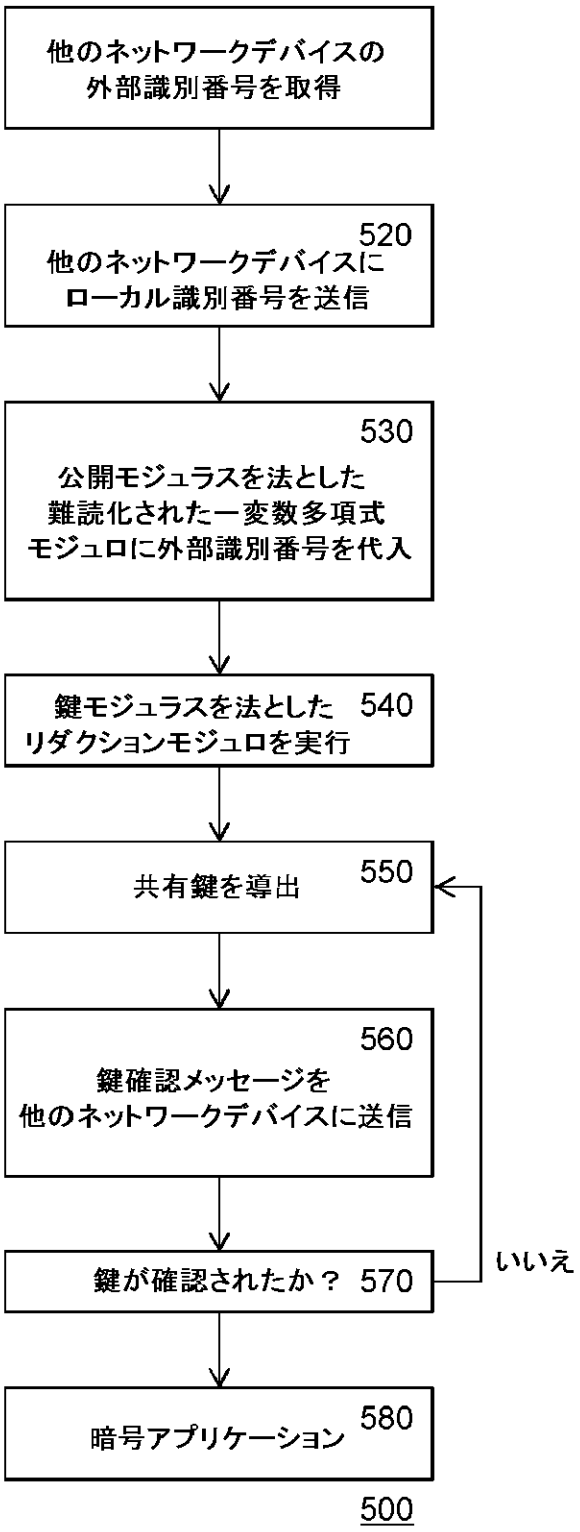

図５

【手続補正書】
【提出日】平成25年8月20日(2013.8.20)
【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】
鍵共有のためにネットワークデバイスを構成する方法であって、前記方法は、
秘密モジュラス、公開モジュラス、及び整数の係数を有する二変数多項式を電子形式で取得する取得ステップであって、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、取得ステップと、
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生成ステップであって、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、前記代入の結果に前記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ことにより前記二変数多項式から一変数多項式を決定するステップとを含む、生成ステップと、
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保存ステップと、前記公開モジュラスを前記ネットワークデバイスに保存する保存ステップと、
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生成ステップは、難読化数を生成するステップと、多項式操作デバイスを使用して、前記難読化数を前記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】
前記二変数多項式は対称多項式である、請求項１又は２に記載の方法。
【請求項４】
前記公開モジュラスのバイナリ表現の最下位の前記鍵長ビットは、前記秘密モジュラスの最下位の前記鍵長ビットと同じである、請求項１乃至３のいずれか一項に記載の方法。
【請求項５】
電子乱数生成部を使用して前記秘密モジュラスを生成するステップと、
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って、電子乱数生成部を使用して前記二変数多項式を生成するステップと
を含む、請求項１乃至４のいずれか一項に記載の方法。
【請求項６】
前記公開モジュラスは$2^{(a+2)b-1} \leq N$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５のいずれか一項に記載の方法。
【請求項７】
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と、秘密モジュラスを法とした係数モジュロを有する複数の二変数多項式とを取得するステップを含み、
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、それぞれの対称二変数多項式に前記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、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６のいずれか一項に記載の方法。
【請求項８】
前記難読化数は、

$$|\varepsilon_{A,i}| < 2^{(a+1-i)b}$$

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７のいずれか一項に記載の方法。

【請求項９】

請求項１に記載の鍵共有のためにネットワークを構成する方法によって構成された第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であって、前記方法は、

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、任意で難読化されていてもよい一変数多項式を含む、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、

前記第２のネットワークデバイスの前記識別番号を前記任意で難読化されていてもよい一変数多項式に代入するステップと、

前記代入の結果に前記公開モジュラスを法としたリダクションモジュロを行い、鍵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、

前記鍵モジュラスを法とした前記リダクションモジュロ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１０】

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、前記鍵モジュラスを法とした前記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を更に含む、請求項９に記載の方法。

【請求項１１】

前記代入の結果前記公開モジュラスを法としたモジュロを、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を更に含み、前記０ビット列除数は１より大きい、請求項９又は１０に記載の方法。

【請求項１２】

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、前記システムは、

秘密モジュラス、公開モジュラス、及び整数の係数を有する対称二変数多項式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が、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し、前記公開モジュラスを前記ネットワークデバイス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、前記代入の結果に前記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ことによって前記二変数多項式から一変数多項式を決定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１３】

請求項１に記載のように暗号鍵である共有鍵を決定するための第１のネットワークデバイスであって、前記第１のネットワークデバイスは、

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任意で難読化されていてもよい一変数多項式を含む、ローカルキー材料取得部と、

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ための受信機と、
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任意で難読化されていてもよい一変数多項式に代入し、前記代入の結果に前記公開モジュラスを法としたリダクションモジュロを行い鍵モジュラスを法としたリダクションモジュロを行うための多項式操作デバイスと、
前記鍵モジュラスを法とした前記リダクションモジュロ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、第１のネットワークデバイス。
【請求項１４】
コンピュータ上で実行されたとき、請求項１乃至１１のいずれか一項に記載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コンピュータプログラム。
【請求項１５】
コンピュータ読み取り可能媒体に取り込まれた請求項１４に記載のコンピュータプログラム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/056730

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SONG GUO ET AL: "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), pages 1-5, XP031703040, ISBN: 978-1-4244-6402-9	1,9, 12-14
A	page 2, left-hand column, 12th line from below - page 2, right-hand column, line 8 page 2, right-hand column, 11th line from below - page 3, left-hand column, line 20 Section IV.	2-8,10, 11,15
	----- -/--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 April 2013	10/05/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/056730

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/149850 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; PHILIPS CORP [US]; GARCIA OSCAR []) 27 December 2007 (2007-12-27)	1,9, 12-14
A	abstract; claims 1,11,19,20,24-26 page 6, line 1 - page 7, line 4 page 8, line 21 - page 9, line 16	2-8,10, 11,15
A	WO 2010/106496 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; GARCIA MORCHON OSCAR [DE]; ERDMAN) 23 September 2010 (2010-09-23) abstract; claims 1,2,4-6 page 3, line 20 - page 4, line 3 page 4, line 18 - line 21 page 13, line 13 - page 18, line 22 page 20, line 5 - line 14 page 22, line 11 - line 14	1-15
A	CHANJUN YANG, JIANMING ZHOU, WENSHENG ZHANG, JOHNNY WONG: "Pairwise Key Establishment for Large-scale Sensor Networks: from Identifier-based to Location-based", ACM, 2 PENN PLAZA, SUITE 701 - NEW YORK USA, 29 May 2006 (2006-05-29), - 1 June 2006 (2006-06-01), XP040043920, Hong Kong Chapter III, section B.	1-15
A	WO 95/05712 A2 (LEIGHTON FRANK THOMSON [US]; MICALI SILVIO [US]) 23 February 1995 (1995-02-23) abstract; claims 1,4,11,14,16 page 7, line 31 - page 8, line 21 page 13, line 6 - page 14, line 2	1-15
A	WO 2010/032161 A1 (PHILIPS INTELLECTUAL PROPERTY [DE]; KONINKL PHILIPS ELECTRONICS NV [NL]) 25 March 2010 (2010-03-25) cited in the application abstract; claim 1 page 2, line 22 - page 3, line 8	1-15

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/056730

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007149850 A2	27-12-2007	CN 101473626 A	01-07-2009
		EP 2036300 A2	18-03-2009
		JP 2009542118 A	26-11-2009
		RU 2009101908 A	27-07-2010
		US 2009129599 A1	21-05-2009
		WO 2007149850 A2	27-12-2007
WO 2010106496 A1	23-09-2010	CN 102356597 A	15-02-2012
		EP 2409453 A1	25-01-2012
		JP 2012521136 A	10-09-2012
		KR 20110129961 A	02-12-2011
		US 2011317838 A1	29-12-2011
		WO 2010106496 A1	23-09-2010
WO 9505712 A2	23-02-1995	CA 2169449 A1	23-02-1995
		US 5519778 A	21-05-1996
		WO 9505712 A2	23-02-1995
WO 2010032161 A1	25-03-2010	CN 102160324 A	17-08-2011
		EP 2359521 A1	24-08-2011
		JP 2012503399 A	02-02-2012
		KR 20110069103 A	22-06-2011
		RU 2011115207 A	27-10-2012
		US 2011167273 A1	07-07-2011
		WO 2010032161 A1	25-03-2010

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

(特許庁注：以下のものは登録商標)
１．ＺＩＧＢＥＥ

(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 ビルディング 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 ビルディング 5
(72)発明者 クマル サンディープ シャンカラン
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 ビルディング 5
(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 ビルディング 5

Ｆターム(参考) 5J104 AA16 AA18 AA32 AA41 EA04 EA18 JA03 NA02 NA36 NA37
PA07