(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2015-521003
(P2015-521003A)
(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

審査請求 未請求　予備審査請求 未請求　（全 38 頁）

(21)出願番号	特願2015-513298 (P2015-513298)
(86)(22)出願日	平成25年4月24日 (2013.4.24)
(85)翻訳文提出日	平成26年12月2日 (2014.12.2)
(86)国際出願番号	PCT/IB2013/053224
(87)国際公開番号	WO2013/175324
(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	61/732,997
(32)優先日	平成24年12月4日 (2012.12.4)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	12196092.6
(32)優先日	平成24年12月7日 (2012.12.7)
(33)優先権主張国	欧州特許庁 (EP)

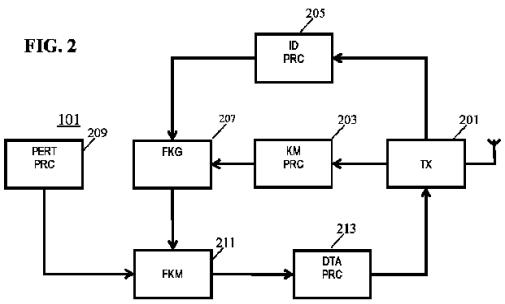
(71)出願人　590000248
コーニンクレッカ　フィリップス　エヌヴェ
オランダ国　５６５６　アーエー　アインドーフェン　ハイテック　キャンパス　５
(74)代理人　110001690
特許業務法人M&Ｓパートナーズ
(72)発明者　ガルシア　モーション　オスカー
オランダ国　５６５６　アーエー　アインドーフェン　ハイ　テック　キャンパス　ビルディング　５

最終頁に続く

(54)【発明の名称】暗号鍵の決定

(57)【要約】
第１の通信ユニット１０１は、信頼できる第３者機関ＴＴＰから第１の鍵生成関数を定めるローカルキー材料を取得するためのプロセッサ２０３を備える。識別子プロセッサ２０５は第２の通信ユニット１０３の識別子を取得し、鍵生成部２０７が識別子に基づいて第１の鍵生成関数から第１の暗号鍵を決定する。生成部２０９は、ＴＴＰに由来するデータによってユニークに決定されない摂動値をローカルに生成する。鍵変更部２１１は、摂動値を第１の暗号鍵に適用することによって共有暗号鍵を決定する。また、第２の通信ユニット１０３も鍵変更データを取得し、それを用いて第１の通信ユニット１０１のための暗号鍵を決定する。その後、第２の通信ユニットは可能な摂動値の値を生成し、更に可能な共有暗号鍵を生成する。その後、第２の通信ユニットは第１の通信ユニット１０１からの暗号データにマッチするものを選択する。摂動値は結託攻撃に対する耐性を高め得る。

FIG. 2



【特許請求の範囲】
【請求項１】
第１の通信ユニットの動作方法であって、前記方法は、
－前記第１の通信ユニットのローカルキー材料を取得するステップであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第１の鍵生成関数を定める、ステップと、
－前記第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するステップと、
－前記識別子に基づいて前記第１の鍵生成関数から第１の暗号鍵を決定するステップと、
－前記第１の暗号鍵の摂動値をローカルに生成するステップであって、前記摂動値は前記信頼できる第３者機関に由来するデータによってユニークに決定されない、ステップと、
－前記摂動値を前記第１の暗号鍵に適用することによって第２の暗号鍵を決定するステップと
を含む、方法。
【請求項２】
前記第２の暗号鍵を用いてデータを生成するステップと、
前記データを前記第２の通信ユニットに伝送するステップと
を更に含む、請求項１に記載の方法。
【請求項３】
ローカルに生成する前記ステップは、前記第２の通信ユニットの識別子に応じて前記摂動値を生成するステップを含む、請求項１に記載の方法。
【請求項４】
前記摂動値をローカルに生成する前記ステップは、前記第２の通信ユニットの識別子の関数として前記摂動値を決定するステップを含む、請求項３に記載の方法。
【請求項５】
前記摂動値は、ある確率分布の乱数値として生成される、請求項１に記載の方法。
【請求項６】
前記確率分布は前記第１の通信ユニットの秘密である、請求項５に記載の方法。
【請求項７】
前記摂動値の大きさは、前記第１の暗号鍵の大きさの１０％以下である、請求項１に記載の方法。
【請求項８】
前記第２の暗号鍵は、前記第１の暗号鍵と前記摂動値とのモジュラ組み合わせによって生成され、前記モジュラ組み合わせは公開モジュラス値を用いる、請求項１に記載の方法。
【請求項９】
第１の通信ユニットの動作方法であって、前記方法は、
－前記第１の通信ユニットのローカルキー材料を取得するステップであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための鍵生成関数を定める、ステップと、
－前記第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するステップと、
－前記第２の通信ユニットの前記識別子に基づき前記鍵生成関数から第１の暗号鍵を決定するステップと、
－前記第２の通信ユニットからデータを受信するステップであって、前記データは第３の暗号鍵を用いて生成され、前記第３の暗号鍵は、摂動値と前記第１の通信ユニットの識別子に依存する暗号鍵との組み合わせである、ステップと、
－前記第２の通信ユニットのための可能な摂動値のセットを決定するステップと、
－前記可能な摂動値のセット及び前記第１の暗号鍵から可能な暗号鍵のセットを決定するステップと、

－前記可能な暗号鍵のセットからの各暗号鍵を用いて前記データに関して暗号演算を行い、共有暗号鍵を、前記暗号演算の有効性基準を満たす前記可能な暗号鍵のセットの暗号鍵として選択することにより、前記第２の通信ユニットのための前記共有暗号鍵を選択するステップと
を含む、方法。
【請求項１０】
前記可能な暗号鍵のセットを決定する前記ステップは、更に、前記第１の暗号鍵と前記第１の通信ユニットの識別子に依存する暗号鍵との間の可能な非対称性に応じて前記可能な暗号鍵を決定するステップを含む、請求項９に記載の方法。
【請求項１１】
複数の通信ユニットを含む通信システムの動作方法であって、前記方法は、第１の通信ユニットが、
－前記第１の通信ユニットのローカルキー材料を取得するステップであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための鍵生成関数を定める、ステップと、
－前記第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するステップと、
－前記識別子に基づき前記第１の鍵生成関数から第１の暗号鍵を決定するステップと、
－前記第１の暗号鍵の摂動値をローカルに生成するステップであって、前記摂動値は前記信頼できる第３者機関に由来するデータによってユニークに決定されない、ステップと、
－前記摂動値を前記第１の暗号鍵に適用することによって第２の暗号鍵を決定するステップと、
－前記第２の暗号鍵を用いてデータを生成するステップと、
－前記データを前記第２の通信ユニットに伝送するステップと
を実行することを含み、更に、前記第２の通信ユニットが、
－前記第２の通信ユニットのローカルキー材料を取得するステップであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第２の鍵生成関数を定める、ステップと、
－前記第１の通信ユニットの識別子を取得するステップと、
－前記第１の通信ユニットの識別子に基づいて前記第２の鍵生成関数から第３の暗号鍵を決定するステップと、
－前記第１の通信ユニットから前記データを受信するステップと、
－前記第１の通信ユニットの可能な摂動値のセットを決定するステップと、
－前記可能な摂動値のセットを前記第３の暗号鍵に適用することによって可能な暗号鍵のセットを決定するステップと
－前記可能な暗号鍵のセットの各暗号鍵を用いて前記データに関して暗号演算を行い、共有暗号鍵を、前記暗号演算の有効性基準を満たす前記可能な暗号鍵のセットの暗号鍵として選択することにより、前記第１の通信ユニットの前記共有暗号鍵を選択するステップとを実行することを含む、方法。
【請求項１２】
－通信ユニットのローカルキー材料を取得するためのプロセッサであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第１の鍵生成関数を定める、プロセッサと、
－異なる通信ユニットの識別子を取得するためのプロセッサと、
－前記識別子に基づき前記第１の鍵生成関数から第１の暗号鍵を決定するためのプロセッサと、
－前記第１の暗号鍵の摂動値をローカルに生成するための生成部であって、前記摂動値は、前記信頼できる第３者機関に由来するデータによってユニークに決定されない、生成部と、
－前記摂動値を前記第１の暗号鍵に適用することによって第２の暗号鍵を決定するための

プロセッサと
を含む、通信ユニット。
【請求項１３】
－通信ユニットのローカルキー材料を取得するためのプロセッサであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための鍵生成関数を定める、プロセッサと、
－異なる通信ユニットの識別子を取得するためのプロセッサと、
－前記異なる通信ユニットの識別子に基づき前記鍵生成関数から第１の暗号鍵を決定するためのプロセッサと、
－前記異なる通信ユニットからデータを受信するための受信機であって、前記データは第３の暗号鍵を用いて生成され、前記第３の暗号鍵は、摂動値と前記第１の通信ユニットの識別子に依存する暗号鍵との組み合わせである、受信機と、
－前記異なる通信ユニットの可能な摂動値のセットを決定するためのプロセッサと、
－前記可能な摂動値のセット及び前記第１の暗号鍵から可能な暗号鍵のセットを決定するためのプロセッサと、
－前記可能な暗号鍵のセットからの各暗号鍵を用いて前記データに関して暗号演算を行い、共有暗号鍵を、前記暗号演算の有効性基準を満たす前記可能な暗号鍵のセットの暗号鍵として選択することにより、前記第２の通信ユニットの共有暗号鍵を選択するための選択部と
を含む、通信ユニット。
【請求項１４】
第１の通信ユニットと第２の通信ユニットとを含む通信システムであって、
前記第１の通信ユニットは、
－前記第１の通信ユニットのローカルキー材料を取得するためのプロセッサであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第１の鍵生成関数を定める、プロセッサと、
－前記第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するためのプロセッサと、
－前記第２の通信ユニットの識別子に基づき前記第１の鍵生成関数から第１の暗号鍵を決定するためのプロセッサと、
－前記第１の暗号鍵の摂動値をローカルに生成するための生成部であって、前記摂動値は、前記信頼できる第３者機関に由来するデータによってユニークに決定されない、生成部と、
－前記摂動値を前記第１の暗号鍵に適用することによって第２の暗号鍵を決定するためのプロセッサと、
－前記第２の暗号鍵を用いてデータを生成するためのデータ生成部と、
－前記データを前記第２の通信ユニットに伝送するための送信部と
を含み、
前記第２の通信ユニットは、
－前記第２の通信ユニットのローカルキー材料を取得するためのプロセッサであって、前記ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第２の鍵生成関数を定める、プロセッサと、
－前記第１の通信ユニットの識別子を取得するためのプロセッサと、
－前記第１の通信ユニットの識別子に基づき前記第２の鍵生成関数から第３の暗号鍵を決定するためのプロセッサと、
－前記第１の通信ユニットから前記データを受信するための受信部と、
－前記第１の通信ユニットのための可能な摂動値のセットを決定するためのプロセッサと、
－前記可能な摂動値のセットを前記第３の暗号鍵に適用することによって可能な暗号鍵のセットを決定するためのプロセッサと、

－前記可能な暗号鍵のセットの各暗号鍵を用いて前記データに関して暗号演算を行い、共有暗号鍵を、前記暗号演算の有効性基準を満たす前記可能な暗号鍵のセットの暗号鍵として選択することにより、前記第１の通信ユニットの前記共有暗号鍵を選択するためのプロセッサと
を含む、通信システム。
【請求項１５】
コンピュータ上で実行されたとき、請求項１乃至１０のいずれか一項に記載の方法の全てのステップを実行する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１６】
コンピュータ読み取り可能媒体上に具現化された請求項１５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】
本発明は暗号鍵の決定に関連し、特に、信頼できる権限からのローカルキー材料に基づく共有鍵に関連する。
【背景技術】
【０００２】
通信システムはユビキタス化しており、有線及び無線システムの両方、更にプライベート及びパブリックネットワークを含む。例えば、広く普及している無線通信規格のセットの１つはＷｉ－Ｆｉ系の通信規格であり、例えば、無線ネットワーキング及びインターネットアクセスを提供するために多くの家庭で利用されている。Ｗｉ－Ｆｉ系の通信規格は、ＩＥＥＥ（Institute of Electrical and Electronic Engineers）によって定められ、普及しているＩＥＥＥ　８０２．１１ａ、ＩＥＥＥ　８０２．１１ｂ、ＩＥＥＥ　８０２．１１ｇ、及びＩＥＥＥ　８０２．１１ｎ規格を含む。Ｗｉ－Ｆｉは更にショップ、ホテル、レストラン等でインターネットワークアクセスを提供するために幅広く利用されている。
【０００３】
多くの通信システム及びアプリケーションにとって重要な特徴の１つは、安全なプライベート／秘密通信をサポートできることである。セキュリティに関する考慮事項は、通信を対象の機関によってのみ復号可能にするという要求を含む。すなわち、通信アプローチは他の機関によって傍受及び復号できない機密通信をサポートすることを要求される。また、情報が正しいソースから受信されたことを確実にする、すなわち、受信データが適切に認証されるという要求も含まれる。セキュリティに関する考慮事項は、更に、通信が例えば対象の機関を装う第３者ではなく、対象の機関同士の間で起こることを確実にするという要求を含む。かかるセキュリティは、第３者がＯＴＡ通信を傍受できないこと、すなわち、第３者が無線伝送を受信してデータの抽出復号に成功できないことを保証することが好ましい。
【０００４】
安全な通信を提供するために、データ伝送は暗号化され得る。しかし、データを暗号化するためには、２つのデバイスが使用される暗号鍵を安全に確立できなければならない。この暗号鍵が対象の機関によってのみ知られることは重要である。
【０００５】
多くの通信システムが、適切な鍵を決定するために各デバイスにおいて使用され得る暗号化情報を提供する信頼機関（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）を使用する。信頼機関はセキュアであり、また、配信が厳しく管理され、信頼できる暗号データを提供するとみなされる。これは、典型的には、システムのインテグリティ及びセキュリティを委任された信用できる団体が信頼機関を運用することを保証する管理システムを実施することによって保証される。

【０００６】
多くのシステムでは、信頼機関はデバイスによって使用される個別の暗号鍵を供給せず、各デバイスが暗号鍵を生成するためのアプローチを確立することを可能にする鍵材料を供給する。例えば、信頼機関は、暗号鍵を計算する方法を指定するデータを第１のデバイスに伝送し得る。データは、例えば、第１のデバイスが安全な通信を確立することを望む他のデバイスの識別子の関数として暗号鍵を生成する方法を定める暗号関数を定め得る。
【０００７】
信頼機関は、各デバイスが受信データ及び所与のデバイスの識別子に基づいて暗号鍵をローカルに生成できるよう、信頼機関は複数のデバイスにデータを送信する。また、関数は対称であるように選択される。すなわち、デバイスＡの関数はデバイスＢの識別子に基づき、デバイスＢがデバイスＡの識別子を用いて計算する暗号鍵と同一な暗号鍵を計算する。したがって、デバイスＡにおいて暗号鍵を生成するための関数がK_Aと表され、デバイスＢにおいて暗号鍵を生成するための関数がK_Bと表される場合、K_A（Ｂ）＝K_B（Ａ）である。
【０００８】
このように、２つのデバイスは信頼機関から受信された情報に基づいて同じ暗号鍵を独自に計算する。
【０００９】
関数は、信頼機関から鍵材料が供給されるデバイスによってのみその関数が知られるよう、安全に配信される。また、関数は、結果の鍵から関数を導出することができないよう、例えば、鍵K_A（Ｂ）の知得から又は同等に（同じ）鍵K_B（Ａ）の知得から関数K_Aを決定することができないよう、導出される。したがって、デバイスは公開情報から各デバイスが使用する関数を計算することはできない。よって、たとえ識別子Ａ及びＢが知られたとしても、第３のデバイスＣは関数K_A又はK_Bのいずれも決定することができず、したがって共有暗号鍵K_A（Ｂ）＝K_B（Ａ）を決定することもできない。
【００１０】
しかし、このアプローチの問題は、攻撃を受ける所与のデバイスについて十分な暗号鍵のサンプルが知られる場合、第３者が根本的な鍵生成関数を決定できないことを保証できないということである。例えば、攻撃者が複数のデバイスからの関数を組み合わせて他のデバイスのための暗号鍵を生成するいわゆる結託攻撃が試みられる場合、そのデバイスが使用する根本的な関数を決定できる可能性がある。例えば、複数のデバイスについて計算された共有鍵、例えばK_C（Ａ）、K_D（Ａ）、K_E（Ａ）、K_F（Ａ）等に関する情報が入手可能である場合、知られている鍵の数が十分に多ければ、K_Aを決定できる可能性がある。
【００１１】
特定の例として、デバイスＡによって使用される関数K_Aに関する情報を取得しようとする起こり得る攻撃を説明する。この例では、攻撃者は識別子B_1，B_2，．．．，B_mの複数の不正アクセスされたデバイスを利用する。攻撃者はこれらのデバイスのそれぞれの秘密鍵生成関数を知っている。デバイスＡとデバイスB_iとの間で通信がイニシャライズされるとき、攻撃者はいつでも上述のように（すなわち、K_{B_i}（Ａ）を決定することによって）K_A（B_i）を取得することができる。この例では、関数K_Aは多項式であり、これはK_Aが比較的低いｍの値、すなわち、多項式K_Aの次数より１大きいｍで復元できることを意味する。この攻撃を防ぐために、非常に大きいｍを選択することができる。しかし、これはK_Aの評価の複雑さを著しく高め、これはメモリが限られたデバイスにとって、又は計算速度が関連する場合に問題になり得る。特定の例として、K_Aの形式が$K_A(x)=<<f_A(x)>_N>_2^b$の場合（f_Aは既知の次数の多項式、$<a>_N$はＮによる除算後の剰余）、f_Aの次数αとｂの相対値に基づいてf_Aを取得することも可能である。特に、$a<\sqrt{b}$の場合、格子基底縮小を用いてf_Aを復元することができ、これにより結果としてK_Aが決定され、システムのセキュリティが破られる。
【００１２】

これは、http://eprint.iacr.org/2012/618.pdfとして入手可能なO.Garcia-Morchon、L. Tolhuizen、D. Gomez、及びJ. Gutierrezによる“Towards fully collusion-resistant ID-based establishment of pairwise keys”, Report 2012/618 at the Cryptology Preprint Archiveにおいて発明者によって詳細に説明されている。

【００１３】

したがって、他のデバイスペアによって生成される鍵に関する情報を突き止めるために複数のデバイスが結託する（又は攻撃者によって利用される）攻撃に対するより高いレジリエンスは望ましかろう。

【００１４】

よって、改良されたアプローチは有益であり、特に、向上されたフレキシビリティ、低減された複雑さ、向上されたセキュリティ、多くの実施されているセキュリティアプローチとの互換性、及び／又は改良されたパフォーマンスを可能にするアプローチは有益であろう。

【発明の概要】

【発明が解決しようとする課題】

【００１５】

したがって、本発明は、上記欠点の１つ以上を個別に又は任意の組み合わせで好適に緩和、軽減、又は排除することを試みる。

【課題を解決するための手段】

【００１６】

本発明の一側面によれば、第１の通信ユニットの動作方法が提供され、前記方法は、第１の通信ユニットのローカルキー材料を取得するステップであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第１の鍵生成関数を定める、ステップと、第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するステップと、識別子に基づいて第１の鍵生成関数から第１の暗号鍵を決定するステップと、第１の暗号鍵の摂動値をローカルに生成するステップであって、摂動値は信頼できる第３者機関に由来するデータによってユニークに決定されない、ステップと、摂動値を第１の暗号鍵に適用することによって第２の暗号鍵を決定するステップとを含む。

【００１７】

本発明は、２つ以上の通信ユニット間の通信のセキュリティを向上させることを可能にし得る。特に、結託攻撃に対するセンシティビティの低減を達成することができる。摂動値は、共有暗号鍵と、完全に対称な鍵生成関数に対応する鍵との間の関係に（場合によっては付加的な）不確実性を導入し得る。この不確実性は、第１の鍵生成関数から導出された共有鍵から第１の鍵生成関数を決定しようとするあらゆる結託第３者機関に対して不確実性を増す。したがって、導出は異なる識別子に対する複数の導出された鍵の考慮を含み、可能な摂動値の多様性は不確実性を著しく高め、通常、第１の鍵生成関数を決定する結託攻撃の実行を事実上不可能にする。

【００１８】

第２の暗号鍵は共有暗号鍵として使用されてもよく、例えば、第１の通信ユニットと第２の通信ユニットとの間の安全な通信のための共有暗号鍵として、及び／又は、例えば暗号ハッシュを用いるデータの暗号認証のための共有暗号鍵として使用され得る。

【００１９】

第１の鍵生成関数は、通信ユニットのための鍵生成関数のセットに属し、鍵生成関数の少なくとも一部のペアは非対称である。鍵生成関数のペア間の非対称性は、例えば、非対称鍵生成関数のペアから生成された暗号鍵間の最大差又は有限個の差等、所定の特性を有し得る。かかる特性は、非対称な鍵生成関数のペアから生成された暗号鍵に基づく共有鍵の決定を容易にし得る。特に、第１の鍵生成関数は、ペアワイズにほぼ対称な関数のセットからの関数であり、例えば、非対称性は、対応する暗号鍵の差が閾値未満になるよう制限されており、閾値は、例えば鍵の値の１％、２％、５％、又は１０％である。

【００２０】
特に、第１の生成関数は、異なる難読化値によってオフセットされた対称な鍵生成関数のセットに対応する非対称な鍵生成関数のセットに属し得る。難読化値の最大値は、例えば、鍵の最大値の１％、２％、５％、又は１０％に制限され得る。特に、ＴＴＰは、まず対称な鍵生成関数のセットを決定し、その後（ランダムであり得る）難読化値を各鍵生成関数に加えることによって鍵生成関数のセットを生成し得る。加算は、例えばモジュラ加算であり得る。

【００２１】
第１の鍵生成関数から生成された各鍵に摂動値を導入することにより、付加的な不確実性が導入される。特に、２つの通信ユニット内で鍵生成関数のセットからの鍵生成関数を使用して生成される鍵の間に付加的な非対称性が導入される。更に、通信ユニットは、生成された暗号鍵の差がＴＴＰによって定められた根本的な鍵生成関数の非対称性、又は摂動値によって導入された非対称性のどちらに起因するのか、又はその割合を決定することができない。鍵生成関数の非対称性は一定であり得るが、摂動値は、例えば通信ユニット間（異なる識別子）で及び／又は鍵確立オペレーションごとに異なり得る。通信ユニットはこれらを区別することができないので、鍵生成関数間の関係は難読化される。

【００２２】
例えば、完全に対称な鍵生成関数に異なる難読化値を加えることによって鍵生成関数が生成される場合、得られる鍵は、ＴＴＰによって導入された難読化値及び通信ユニットによって導入された摂動値の和である値によってオフセットされた根本的な対称関数に対応し得る。難読化値は、しばしば所与の通信ユニット／鍵生成関数に関して一定であり得る。摂動値は通信ユニットによってローカルに生成され、他の通信ユニット（及びＴＴＰ）に対して少なくとも部分的に未知である。他の通信ユニットは、せいぜい、受信された鍵と自身のローカルキー生成関数から生成された鍵との差を決定できる程度である。結合された差は、２つの鍵生成関数の難読化値、及び摂動値の和に対応する。しかし、通信ユニットは結合された差を個別の部分に分離することができず、よって摂動値の効果を取り除くことができない。したがって、確立された暗号鍵の知識から第１の鍵生成関数を決定しようと試みる場合、攻撃結託通信ユニットは通信ユニットごとに第１の鍵生成関数によって生成された値を決定することができず、摂動値の不確実性に対応する複数の可能な値を生成することしかできない。したがって、各鍵確立は、攻撃通信ユニットが決定しようとしている鍵生成関数の結果の１つのサンプルを提供せず、せいぜい、鍵生成関数によって生成された複数の可能な鍵のセットを提供するだけである。第１の鍵生成関数を決定するためには複数の通信ユニットの結果を解析しなければならないので、要求される複雑性は各通信ユニットの可能な鍵の数の積とともに、すなわち、各鍵確立において使用された可能性がある可能な摂動値の組み合わせの数とともに上昇する。この複雑性は、結託攻撃を事実上非現実的にする。

【００２３】
ローカルキー材料は第１の鍵生成関数をユニークに定め得る。摂動値はＴＴＰから受信される情報にユニークに依存しない。したがって、共有鍵はＴＴＰによってユニークに決定されない。したがって、他の通信ユニットは、生成鍵が静的な関数からユニークに与えられると仮定することができない。したがって、攻撃結託通信ユニットは、異なる通信ユニットからの結果を組み合わせるとき、摂動値の全ての可能な値を考慮しなければならない。

【００２４】
摂動値は、少なくとも一部の共有鍵確立間で異なり、例えば、同じ通信ユニット間の通信のための異なる鍵確立ごとに、又は、異なる通信ユニット間の通信のための異なる鍵確立ごとに異なり得る。

【００２５】
摂動値を生成するためのプロセスは第１の通信ユニットの機密／秘密であり得る。摂動値は、第１の通信ユニットの外部では入手できないデータに少なくとも部分的に基づいて

生成されてもよい。多くの実施形態では、摂動値はランダム要素を含み得る。摂動値は、ローカルキー材料から独立して決定されてもよい。

【００２６】

ＴＴＰは中央暗号サーバ又はネットワーク権限であり得る。第１の鍵生成関数は、識別子の一変数関数であり得る。摂動値は、少なくとも一部の鍵確立において非ゼロである。

【００２７】

ＴＴＰは、第１の通信ユニットを鍵共有のために構成する方法を実行するよう構成され、方法は、秘密モジュラス（p_1）、公開モジュラス（Ｎ）、及び整数係数を有する二変数多項式（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、第１の通信ユニットの識別番号（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、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秘密モジュラス（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第１の通信ユニットに電子的に保存するステップとを含む。

【００２８】

第１の通信ユニットのローカルキー材料を生成するステップは、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。二変数多項式（f_1）は対称多項式であり得る。

【００２９】

一部の実施形態では、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。一部の実施形態では、一変数多項式の各係数に難読化数が加えられる。

【００３０】

難読化数及び／又は摂動値は正数に限定され得るが、これは必須ではなく、値は負でもよい。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が得られてもよい。このようにして、一変数多項式の１以上の係数、好ましくは更に全ての係数が難読化されてもよい。

【００３１】

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定め、第１の鍵生成関数の演算は、任意で難読化されていてもよい一変数多項式に第２の通信デバイスの識別子を代入し、代入の結果を公開モジュラスを法としたモジュロによりリダクションし、鍵モジュラスを法としたモジュロによりリダクションし、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第１の暗号鍵を導出することを含み得る。

【００３２】

かかる例では、ローカルキー材料は通常ほぼ対称な多項式から得られ、これは、通信ユニットペアが同じ共有鍵を取得することを可能にする。ローカルキー材料に難読化数が加えられるので、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、すなわち、完全な対称性はもはや存在しない。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。
【００３３】
アプローチは、例えば、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つを使用する通信ユニットは識別子に関連付けられる。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プロプライエタリビット列でもよい。
【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。共有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共有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つを利用できるデバイスのみが通信を解読できる。共有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つを利用できるデバイスのみが認証メッセージを作成できる。
【００３５】
本発明のオプションの特徴によれば、方法は更に、第２の暗号鍵を用いてデータを生成するステップと、データを第２の通信ユニットに伝送するステップとを含む。
【００３６】
これは、第２の通信ユニットが共有鍵を決定することを可能にし得る。データは、例えば、第２の暗号鍵を用いて暗号化されたデータであり、且つ／又は、例えば第２の暗号鍵を用いて生成された暗号ハッシュであり得る。
【００３７】
本発明のオプションの特徴によれば、生成するステップは、第２の通信ユニットの識別子に応じて摂動値を生成するステップを含む。
【００３８】
これは、多くの実施形態において特に好適な摂動値を提供し得る。特に、一部の実施形態ではセキュリティを高め、例えば、摂動値が通信ユニットごとに異なることを保証し、もって不確実性を高め、結託攻撃を妨げるために使用され得る。
【００３９】
本発明のオプションの特徴によれば、摂動値を決定するステップは、第２の通信ユニットの識別子の関数として摂動値を決定するステップを含む。
【００４０】
これは、多くの実施形態において特に好適な摂動値を与え得る。特に、一部の実施形態ではセキュリティを高め、摂動値が通信ユニットごとに異なることを保証し、もって不確実性を高め、結託攻撃を妨げるために使用され得る。更に、新しい通信セッションごとに新しい共有鍵を決定する必要がないので、複雑さが低減され得る。一部の実施形態では、摂動値は識別子からユニークに決定され得る。
【００４１】
本発明のオプションの特徴によれば、摂動値は、ある確率分布の乱数値として生成される。
【００４２】
これは複雑さの低いアプローチを可能にし、高度な不確実性を導入することにより、結託攻撃を著しく困難にし得る。
【００４３】
確率分布は典型的には摂動値を鍵長に比して比較的小さい値に限定する。
【００４４】
分布は非ゼロ平均を有し得る。

【００４５】
本発明のオプションの特徴によれば、確率分布は第１の通信ユニットの秘密である。
【００４６】
これはセキュリティを高め得る。特に、多くの実施形態では、摂動値を生成するために使用される確率分布は第１の通信ユニットの外部には（完全には）知られない。かかる実施形態では、確率関数の少なくとも１つの特徴は第１の通信ユニットの秘密であり得る。これは、摂動値の効果を推定するために複数の鍵確立及び統計的演算が使用できないことを保証し得る。例えば、攻撃通信ユニットは攻撃通信ユニットによる繰り返しの鍵確立を平均し得る。攻撃ユニットが確率分布の平均を知る場合、ある識別子との繰り返しの鍵確立から生成された複数の第２の暗号鍵を平均し、平均値を差し引くことによって所与の識別子のための第１の暗号鍵を決定することができる。しかし、分布の平均が攻撃ユニットに対して未知の場合、このアプローチを利用することはできない。
【００４７】
本発明のオプションの特徴によれば、摂動値の大きさは、第１の暗号鍵の大きさの１０％以下である。
【００４８】
これは、高度なセキュリティを保証しつつ、第２の通信ユニットにおける計算を容易にし得る。一部の実施形態では、摂動値の値は好適に第１の暗号鍵の値の５％以下、場合によっては１％以下である。
【００４９】
本発明のオプションの特徴によれば、第２の暗号鍵は、第１の暗号鍵と摂動値とのモジュラ組み合わせによって生成され、モジュラ組み合わせは公開モジュラス値を用いる。
【００５０】
これは演算を容易にし得る。公開モジュラスは、特に第２の暗号鍵の長さに対応してもよい。モジュラス組み合わせは、特にモジュラス加算でもよい。
【００５１】
本発明の一側面によれば、第１の通信ユニットの動作方法が提供され、方法は、第１の通信ユニットのローカルキー材料を取得するステップであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための鍵生成関数を定める、ステップと、第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するステップと、第２の通信ユニットの識別子に基づき鍵生成関数から第１の暗号鍵を決定するステップと、第２の通信ユニットからデータを受信するステップであって、データは第３の暗号鍵を用いて生成され、第３の暗号鍵は、摂動値と第１の通信ユニットの識別子に依存する暗号鍵との組み合わせである、ステップと、第２の通信ユニットのための可能な摂動値のセットを決定するステップと、可能な摂動値のセット及び第１の暗号鍵から可能な暗号鍵のセットを決定するステップと、可能な暗号鍵のセットからの各暗号鍵を用いてデータに関して暗号演算を行い、共有暗号鍵を、暗号演算の有効性基準を満たす可能な暗号鍵のセットの暗号鍵として選択することにより、第２の通信ユニットのための共有暗号鍵を選択するステップとを含む。
【００５２】
本発明は、通信ユニットがローカルに生成された鍵に基づいて他の通信ユニットによって用いられた鍵を決定することを可能に又は容易にし得る。上記のコメント、例えば鍵生成関数に関するコメントは、かかる通信ユニットに等しく適用され得ることを理解されたい。
【００５３】
データは、例えば、第３の暗号鍵を用いて暗号化されたデータ、及び／又は、例えば、第３の暗号鍵を用いて生成された暗号ハッシュであり得る。暗号演算は、例えば、可能な暗号鍵のセットからの各暗号鍵を用いてデータを解読することを含み得る。検証基準は解読されたデータの有効性の指標であり得る。暗号演算は、例えば、可能な暗号鍵のセットからの各暗号鍵を用いて暗号ハッシュを生成することを含み得る。検証基準は、生成され

た暗号ハッシュと、データの暗号ハッシュとのマッチングが基準を満たすという条件であり得る。

【００５４】

本発明のオプションの特徴によれば、可能な暗号鍵のセットを決定するステップは、更に、第１の暗号鍵と第１の通信ユニットの識別子に依存する暗号鍵との間の可能な非対称性に応じて可能な暗号鍵を決定するステップを含む。

【００５５】

これは、改良されたオペレーション及びセキュリティを提供し得る。可能な非対称性は、第１の鍵生成関数によって生成された鍵と、データを生成するために使用された第１の通信ユニットの識別子に依存する暗号鍵との間の可能な差のセットによって示され得る。例えば、両鍵間の可能な差の最大値が知られていてもよい。可能な摂動値及び可能な非対称性差に基づき、第１の暗号鍵と第１の通信ユニットの識別子に依存する暗号鍵との間の可能な差の合計が決定され得る。その後、第１の暗号鍵を最大差を超えない値によって変更することによって得られる全ての可能な鍵を生成することにより、可能な暗号鍵を生成することができる。

【００５６】

本発明の一側面によれば、複数の通信ユニットを含む通信システムの動作方法が提供され、方法は、第１の通信ユニットが、第１の通信ユニットのローカルキー材料を取得するステップであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための鍵生成関数を定める、ステップと、第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するステップと、識別子に基づき第１の鍵生成関数から第１の暗号鍵を決定するステップと、第１の暗号鍵の摂動値をローカルに生成するステップであって、摂動値は信頼できる第３者機関に由来するデータによってユニークに決定されない、ステップと、摂動値を第１の暗号鍵に適用することによって第２の暗号鍵を決定するステップと、第２の暗号鍵を用いてデータを生成するステップと、データを第２の通信ユニットに伝送するステップとを実行することを含み、更に、第２の通信ユニットが、第２の通信ユニットのローカルキー材料を取得するステップであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第２の鍵生成関数を定める、ステップと、第１の通信ユニットの識別子を取得するステップと、第１の通信ユニットの識別子に基づいて第２の鍵生成関数から第３の暗号鍵を決定するステップと、第１の通信ユニットからデータを受信するステップと、第１の通信ユニットの可能な摂動値のセットを決定するステップと、可能な摂動値のセットを第３の暗号鍵に適用することによって可能な暗号鍵のセットを決定するステップと可能な暗号鍵のセットの各暗号鍵を用いてデータに関して暗号演算を行い、共有暗号鍵を、暗号演算の有効性基準を満たす可能な暗号鍵のセットの暗号鍵として選択することにより、第１の通信ユニットの共有暗号鍵を選択するステップとを実行することを含む。

【００５７】

本発明の一側面によれば、通信ユニットのローカルキー材料を取得するためのプロセッサであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第１の鍵生成関数を定める、プロセッサと、異なる通信ユニットの識別子を取得するためのプロセッサと、識別子に基づき第１の鍵生成関数から第１の暗号鍵を決定するためのプロセッサと、第１の暗号鍵の摂動値をローカルに生成するための生成部であって、摂動値は、信頼できる第３者機関に由来するデータによってユニークに決定されない、生成部と、摂動値を第１の暗号鍵に適用することによって第２の暗号鍵を決定するためのプロセッサとを含む通信ユニットが提供される。

【００５８】

本発明の一側面によれば、通信ユニットのローカルキー材料を取得するためのプロセッサであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための鍵生成関数を定める、プロセッサと、異なる通

信ユニットの識別子を取得するためのプロセッサと、異なる通信ユニットの識別子に基づき鍵生成関数から第１の暗号鍵を決定するためのプロセッサと、異なる通信ユニットからデータを受信するための受信機であって、データは第３の暗号鍵を用いて生成され、第３の暗号鍵は、摂動値と第１の通信ユニットの識別子に依存する暗号鍵との組み合わせである、受信機と、異なる通信ユニットの可能な摂動値のセットを決定するためのプロセッサと、可能な摂動値のセット及び第１の暗号鍵から可能な暗号鍵のセットを決定するためのプロセッサと、可能な暗号鍵のセットからの各暗号鍵を用いてデータに関して暗号演算を行い、共有暗号鍵を、暗号演算の有効性基準を満たす可能な暗号鍵のセットの暗号鍵として選択することにより、第２の通信ユニットの共有暗号鍵を選択するための選択部とを含む通信ユニットが提供される。

【００５９】

本発明の一側面によれば、第１の通信ユニットと第２の通信ユニットとを含む通信システムが提供され、第１の通信ユニットは、第１の通信ユニットのローカルキー材料を取得するためのプロセッサであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第１の鍵生成関数を定める、プロセッサと、第１の通信ユニットとは異なる第２の通信ユニットの識別子を取得するためのプロセッサと、第２の通信ユニットの識別子に基づき第１の鍵生成関数から第１の暗号鍵を決定するためのプロセッサと、第１の暗号鍵の摂動値をローカルに生成するための生成部であって、摂動値は、信頼できる第３者機関に由来するデータによってユニークに決定されない、生成部と、摂動値を第１の暗号鍵に適用することによって第２の暗号鍵を決定するためのプロセッサと、第２の暗号鍵を用いてデータを生成するためのデータ生成部と、データを第２の通信ユニットに伝送するための送信部とを含み、

第２の通信ユニットは、第２の通信ユニットのローカルキー材料を取得するためのプロセッサであって、ローカルキー材料は、信頼できる第３者機関に由来し、少なくとも１つの識別子の関数として暗号鍵を生成するための第２の鍵生成関数を定める、プロセッサと、第１の通信ユニットの識別子を取得するためのプロセッサと、第１の通信ユニットの識別子に基づき第２の鍵生成関数から第３の暗号鍵を決定するためのプロセッサと、第１の通信ユニットからデータを受信するための受信部と、第１の通信ユニットのための可能な摂動値のセットを決定するためのプロセッサと、可能な摂動値のセットを第３の暗号鍵に適用することによって可能な暗号鍵のセットを決定するためのプロセッサと、可能な暗号鍵のセットの各暗号鍵を用いてデータに関して暗号演算を行い、共有暗号鍵を、暗号演算の有効性基準を満たす可能な暗号鍵のセットの暗号鍵として選択することにより、第１の通信ユニットの共有暗号鍵を選択するためのプロセッサとを含む。

【００６０】

本発明の上記及び他の側面、特徴、及び利点は、下記の実施形態を参照して説明され、明らかになるであろう。

【図面の簡単な説明】

【００６１】

本発明の実施形態を、あくまで例である図面を参照して説明する。

【００６２】

【図１】図１は、複数の通信ユニットを含む通信確立の図である。

【図２】図２は、本発明の一部の実施形態に係る通信ユニットの要素の図である。

【図３】図３は、本発明の一部の実施形態に係る通信ユニットの要素の図である。

【図４】図４は、本発明の一部の実施形態に係る通信ユニットの動作方法の要素の図である。

【図５】図５は、本発明の一部の実施形態に係る通信ユニットの動作方法の要素の図である。

【図６】図６は、通信ネットワークのＴＴＰの要素の図である。

【図７】図７は、通信ネットワークのＴＴＰの要素の図である。

【発明を実施するための形態】

【００６３】
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、いくつか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。
【００６４】
以下の説明は、無線通信システムに適用可能な本発明の実施形態に焦点を当てる。しかし、本発明はこのアプリケーションに限定されず、例えばインターネットを含む完全に又は部分的に有線である通信システムにも適用できることを理解されたい。
【００６５】
図１は、本発明の一部の実施形態に係る無線通信システムの一例を示す。
【００６６】
無線通信システムは、共有暗号鍵を用いてデータを安全且つプライベートに通信しようとする第１の通信ユニット１０１（又はネットワークデバイス）及び第２の通信ユニット１０３（又はネットワークデバイス）を含む。第１の通信ユニット１０１と第２の通信ユニット１０３との間のデータ通信は、具体的にはＷｉ－Ｆｉ通信リンクであり得る無線通信リンクを介して行われる。例えば、第１の通信ユニット１０１又は第２の通信ユニット１０３はＷｉ－Ｆｉアクセスポイントであり、他方のユニットは当該アクセスポイントによってサポートされるモバイル通信ユニットであり得る。
【００６７】
Ｗｉ－Ｆｉ通信リンクは、例えばＩＥＥＥ　８０２．１１ａ、ＩＥＥＥ　８０２．１１ｂ、ＩＥＥＥ　８０２．１１ｇ、ＩＥＥＥ　８０２．１１ｎ、ＩＥＥＥ　８０２．１１ａｃ、及びＩＥＥＥ　８０２．１１ａｄ規格のうちの１つ等のＷｉ－Ｆｉ通信規格の系に適合する通信リンクであり得る。Ｗｉ－Ｆｉ通信リンクは、特にＩＥＥＥ　８０２．１１規格ベースの通信をサポートし得る。
【００６８】
この例では、第１の通信ユニット１０１及び第２の通信ユニット１０３は如何なる第３者によっても取得可能であってはならない機密情報を交換しようとする。このために、第１の通信ユニット１０１及び第２の通信ユニット１０３は通信リンク上で交換されるデータの暗号化を用いる。かかる暗号化を実行するために、第１の通信ユニット１０１及び第２の通信ユニット１０３は共有暗号鍵を使用する。あるいは又は更に、共有暗号鍵は、例えば暗号ハッシュを生成することによって交換データを認証するために使用されてもよい。
【００６９】
図１の例では、一群の通信デバイス１０５が第１の通信ユニット１０１と第２の通信ユニット１０３との間の無線通信を受信できる。この特定の例では、例えば第１の通信ユニット１０１と第２の通信ユニット１０３との間で交換される秘密情報にアクセスするために、一群の通信デバイス１０５は協力して第１の通信ユニット１０１が使用する根本的な鍵生成関数を決定しようとする。したがって、第１の通信ユニット１０１と第２の通信ユニット１０３との間の通信のセキュリティ及び機密性を破るべく、一群のデバイス１０５は情報を共有するよう構成される。また、一群の通信デバイス１０５は、第１の通信ユニット１０１及び／又は第２の通信ユニット１０３と直接安全な通信を確立することによって情報を得ようとする可能性もある。
【００７０】
図１のシステムでは、暗号鍵情報の配信及び管理は、この特定の例では中央暗号サーバであるＴＴＰ１０７によって管理される。ＴＴＰ１０７は、受信通信ユニットによって使用される暗号鍵が如何に計算されるべきかを定めるデータを供給する信頼機関である。したがって、ＴＴＰ１０７はあくまで各通信ユニットが安全な通信のために用いられる暗号鍵を如何にして生成すべきかに関する情報を配信するに過ぎない。ＴＴＰ１０７は、信用され、信頼できると考えられる団体によって管理及び運用される。したがって、ＴＴＰ１０７から受信された鍵材料を信用及び信頼して危険にさらされていない暗号鍵を生成する

ためのアプローチを定めることができるという仮定の下、通信ユニットは動作する。

【００７１】

ＴＴＰ１０７と通信ユニットとの間の通信は、他の通信ユニットが情報にアクセスできないよう、更に安全に実行される。ＴＴＰ１０７から各通信ユニットに鍵材料を安全に配信するためのアプローチは当業者に知られており、簡潔さのために本明細書ではこれ以上説明しない。

【００７２】

図１のシステムでは、ＴＴＰ１０７は、暗号鍵を生成するための関数を定めるローカルキー材料を供給するために通信ユニットと無線通信し得る中央暗号サーバである。他の実施形態では、ローカルキー材料は他の手段によって供給されてもよく、例えば有線通信ネットワークを介して、又はリムーバブルメモリ等の媒体を介して供給されてもよい。他の実施形態では、ローカルキー材料は製造中に提供されて各通信ユニット内に記憶されてもよい（実際には、通信ユニット内にハードワイヤードにされてもよい）。

【００７３】

この例では、通信ユニットに供給される鍵材料は、各通信ユニットが暗号鍵を生成する方法を表す関数をユニークに定める。特に、ローカルキー材料は、暗号鍵を生成する方法のための関数を１つ以上の識別子の関数としてユニークに定める。特に、関数は単一の通信ユニットの識別子から暗号鍵を生成する方法を定め、よって一変数関数であり得る。したがって、所与の通信ユニットＸに供給される鍵材料は、通信ユニットＸが如何にして他の通信ユニットと共に使用するための暗号鍵を導出すべきかを定め、すなわち、関数K_X（Ｙ）を定め得る。

【００７４】

まず、対称関数について、すなわち、配信される鍵材料がペアワイズに対称な関数を定め得る場合について、すなわち、

$$K_X（Y）＝K_Y（X）$$

が全ての通信ユニットのペアについて成立する場合を考察する。

【００７５】

従来、安全に通信しようとしている２つの通信ユニットは、かかる場合、単純に他方の通信ユニットの通信ユニット識別子を用いて各自の暗号生成関数を評価することによって共有暗号鍵を決定し得る。これらのアプローチは個々に同一の鍵をもたらすので、例えばこの共有暗号鍵を用いてデータを暗号化することによって通信を行うことができる。

【００７６】

ＴＴＰ１０７によって定められる鍵生成関数は、一方向に評価することは比較的容易であるが、得られた暗号鍵から求めることは非常に難しいという特性を有する。実際に、たとえ第３者があるユニットの通信ユニット識別子及び対応する暗号鍵を知っていたとしても、使用された根本的な鍵生成関数を決定することはできない。

【００７７】

例えば、一群の攻撃通信デバイス１０５のうちの１つが第１の通信ユニット１０１と安全な通信を確立した場合、そのデバイスは対応する識別子を知り、第１の通信ユニット１０１が自身のローカルキー生成関数及び攻撃通信ユニットの識別子に基づいて生成する暗号鍵にも対応する、その識別子に対する暗号鍵をローカルに決定できる。しかし、攻撃通信ユニットはこの鍵から第１の通信ユニット１０１が使用する根本的な鍵生成関数を決定することはできず、よって第１の通信ユニット１０１が第２の通信ユニット１０３と通信する場合に生成する暗号鍵を決定することはできない。

【００７８】

具体的には、第１の通信ユニット１０１をＡと、第２の通信ユニット１０３をＢと、そして一群の通信デバイス１０５をＣ、Ｄ、Ｅ等と表すと、一群の通信デバイス１０５の１つの通信ユニットはデバイスＡと共有鍵を確立し得る。したがって、そのユニットは鍵Ｋ

$_A$（Ｃ）と同一である鍵Ｋ$_C$（Ａ）を決定し得る。しかし、Ｋ$_A$（Ｃ）を知っていたとしても、攻撃通信ユニット１０５はＫ$_A$（ｘ）を決定することはできない、すなわち、根本的な鍵生成関数を決定することはできない。よって、攻撃通信ユニット１０５は暗号鍵Ｋ$_A$（Ｂ）を決定することもできず、したがって第１の通信ユニット１０１と第２の通信ユニット１０３との間の通信のための共有鍵を決定することはできない。

【００７９】

しかし、複数の通信ユニットがいわゆる結託攻撃を実行すべく協働する場合、攻撃パーティは大幅に多くの情報を集めることができる。例えば、一群の通信デバイス１０５の全ての通信ユニットが第１の通信ユニット１０１についての共有鍵を求める場合、複数の暗号鍵が知られる、すなわち、攻撃パーティはＫ$_A$（Ｃ）、Ｋ$_A$（Ｄ）、Ｋ$_A$（Ｅ）、Ｋ$_A$（Ｆ）等を知る。

【００８０】

かかる共有鍵が十分に知られる場合、一部のシステムでは、鍵生成関数Ｋ$_A$（ｘ）、よって共有鍵Ｋ$_A$（Ｂ）を決定できる可能性があることが示され得る。したがって、一部のシステムでは、結託攻撃によって通信のセキュリティ及び機密性が破られる可能性がある。

【００８１】

システムが通信ユニットにおいて完全に対称であることが保証されず、通常近似的にのみ対称である鍵生成関数を使用する場合、すなわち、Ｘ及びＹの全てのペアについて、

$$K_X(Y) \quad K_Y(X)$$

しか成立しないような場合、アプローチをより難解にすることができる。非対称性は、例えば、完全に対称な対応する関数にある値（難読化値又は難読化数と呼ばれる）を加えることによって導入され得る。例えば、ＴＴＰはペアワイズに対称な関数のセットを決定して、その後これらの関数に異なる難読化値を加えることによって完全には対称でない関数を生成し得る。

【００８２】

かかるアプローチは、結託攻撃通信ユニットが単純にローカルに生成された鍵Ｋ$_C$（Ａ）、Ｋ$_D$（Ａ）、Ｋ$_E$（Ａ）、Ｋ$_F$（Ａ）を第１の鍵生成関数の標本点として、すなわちＫ$_A$（Ｃ）、Ｋ$_A$（Ｄ）、Ｋ$_A$（Ｅ）、Ｋ$_A$（Ｆ）として使用することを防ぐことができる。対応する計算された鍵の間には差異が存在し得るので、Ｋ$_A$（ｘ）を決定するためのアプローチは全ての可能な差異を含むよう拡張されなければならない。これは複雑さを著しく高め、攻撃を非現実的にし得る。

【００８３】

意図された２つの通信デバイスが共有暗号鍵について合意するためには、２つのローカルに生成された共有鍵を合わせるために追加のプロセスを実行しなければならない。かかるシステムの一例は、２０１２年５月２１日に出願された米国出願６１／６４９４６４（整理番号２０１２ＰＦ００７１７）に見つけることができる。このアプローチでは、例えばマッチが見つかるまで暗号鍵のＬＳＢ（least significant bits）を破棄することに基づく反復的通信によって生成された鍵の同一部分を特定して共有鍵を決定するプロセスを使用することができる。これは、非対称鍵生成関数から得られる暗号鍵間の差異を決定することを可能にする。

【００８４】

しかし、一部のシステムでは、通信ユニットが潜在的な攻撃通信ユニットと鍵確立ルーチンを実行し得ないことは保証できない。例えば、一部のシステムでは、あらゆる通信ユニットがあらゆる他の通信ユニットと共有暗号鍵セットアップを開始できる。この場合、攻撃通信ユニットは、ローカルに生成される関数間の差異を決定することができる、すなわち、難読化値の効果が決定され、よって除去され得る。したがって、かかるシナリオでは、各攻撃通信ユニットは、攻撃されている鍵生成関数によって生成された１つの暗号鍵

をやはり決定し得る可能性がある。したがって、完全な対称性の欠如によって導入された不確実性が攻撃通信ユニットによって解かれる可能性がある。

【００８５】

図１のシステムでは、第１の通信ユニット１０１及び第２の通信ユニット１０３は、結託攻撃に対する改良されたロバストネス及びセキュリティを可能にする改変された鍵生成アプローチを使用する。

【００８６】

図２は第１の通信ユニット１０１の要素を示し、図３は第２の通信ユニット１０３の要素を示す。図４は第１の通信ユニット１０１によって共有鍵を決定するための方法の一例を示し、図５は第２の通信ユニット１０３によって共有鍵を決定するための方法の一例を示す。

【００８７】

第１の通信ユニット１０１は、他の通信ユニットのＯＴＡインターフェイスと通信するよう構成された第１の無線送受信機２０１を含む。特に、第１の無線送受信機２０１は無線伝送によってＴＴＰ１０７及び第３の通信ユニット１０５と通信できる。この特定の例では、ＯＴＡ通信はＷｉＦｉ通信であり、よって第１の無線送受信機２０１はＷｉＦｉ通信規格に基づいて動作するよう構成され得る。他の実施形態では、第１の通信ユニット１０１（及び実際には第２の通信ユニット１０３も）ＴＴＰ１０７から有線媒体又はメモリカード等のポータブルメディアを介してデータを受信し得る。他の実施形態では、データ（及び特に鍵材料）は製造中にＴＴＰ１０７によって供給され、また、この時点で通信ユニット内にプログラミングされ得る。

【００８８】

第１の無線送受信機２０１は、ＴＴＰ１０７に由来するローカルキー材料が取得されるステップ４０１を実行する第１の鍵材料プロセッサ２０３に結合される。この特定の例では、ローカルキー材料は（安全な）無線通信によってＴＴＰ１０７から受信されるが、他の実施形態では、内部及び外部ソースの両方を含め、他のソースから取得されてもよいことを理解されたい。例えば、ローカルキー材料は製造中にＴＴＰ１０７によって提供され、第１の通信ユニット１０１のローカルストレージ内に記憶されてもよい。他の例として、着脱可能メモリ（例えば、メモリカード又はＵＳＢ）等の適切なポータブルメディアから提供されてもよい。

【００８９】

ローカルキー材料は、安全な暗号オペレーションをサポートするために要求される暗号鍵を生成するために使用され得る第１の鍵生成関数をユニークに定める。第１の鍵生成関数はその特定の通信ユニットに固有であり、すなわち、第１の通信ユニット１０１の第１の鍵生成関数は他の通信ユニットによって使用される鍵生成関数とは異なる。第１の鍵生成関数は、１つ以上の通信ユニットの識別子（又は、同等に、通信ユニットに関連付けられたユーザの識別子）に基づいて暗号鍵を提供する。

【００９０】

以下の例は、第１の鍵生成関数が、共有鍵が決定される対象の通信ユニットの識別子の一変数関数である実施形態に焦点を当てる。したがって、第１の鍵生成関数は$K_A(x)$として与えられ、ここで、インデックスＡは第１の鍵生成関数を表し、ｘは暗号鍵を生成するための入力識別子を表す。

【００９１】

しかし、一部の実施形態では、第１の鍵生成関数は２つ以上の識別子の関数であり得る。例えば、３つの通信ユニットが単一の共有鍵を使用して３方向の安全な通信を確立する場合、第１の鍵生成関数は、通信に関与する他の通信ユニットの２つの識別子に基づいて暗号鍵を提供できる関数として定められ得る。

【００９２】

この例では、ローカルキー材料は第１の鍵生成関数をユニークに定め、すなわち、ローカルキー材料に基づいて、可能な識別子（又は、第１の鍵生成関数が複数の識別子の関数

の場合、識別子のセット）ごとに暗号鍵がユニークに定められる。この特定の実施形態では、以下でより詳細に述べられるように、ローカルキー材料は暗号鍵を生成するために使用される多項式を定める。

【００９３】

したがって、ステップ４０１において、第１の鍵材料プロセッサ２０３は第１の鍵生成関数をユニークに定めるローカルキー材料を取得する。

【００９４】

第１の通信ユニット１０１は、更に、安全な通信がイニシャライズされようとしている、すなわち、共有暗号鍵が決定されるべき対象の通信ユニットの識別子を第１の通信ユニット１０１が決定するステップ４０３を実行するよう構成される第１の識別子プロセッサ２０５を含む。したがって、この特定の例では、第１の識別子プロセッサ２０５は第２の通信ユニット１０３の識別子を決定するよう構成される。

【００９５】

第２の通信ユニットの識別子は任意の適切な方法で決定され、例えば、第２の通信ユニット１０３自身からの通信確立リクエストに応じて、又は、第１の通信ユニット１０１へのユーザ入力に応じて等によって決定され得ることを理解されたい。

【００９６】

第１の鍵材料プロセッサ２０３及び第１の識別子プロセッサ２０５は、第１の鍵生成関数及び決定された第２の通信ユニット１０３の識別子（識別子Ｂとする）を用いて第１の暗号鍵が決定されるステップ４０５を実行するよう構成される第１の鍵生成部２０７に結合される。したがって、第１の鍵生成部２０７は識別子Ｂを入力として用いて第１の鍵生成関数を計算し、これによって第１の暗号鍵を生成する。すなわち、第１の鍵生成部２０７は値K_A（Ｂ）を計算する。

【００９７】

従来のシステムでは、他方の通信ユニットは独自の鍵生成関数に基づき、第１の通信ユニット１０１の識別子を入力として共有鍵を別に計算し、生成される第１の暗号鍵は典型的には直接共有鍵として使用される。従来のシステムでは鍵生成関数は対称である。一方、この例では、鍵生成関数は非対称ではあるが略対象な関数のセットから選択される。特に鍵生成関数は、対称な鍵生成関数のセットに異なる難読化値を加えることによって生成される関数である。

【００９８】

更に、図１のシステムでは、第１の鍵生成関数によって生成される第１の暗号鍵は共有鍵として使用されず、摂動値がローカルに生成され、典型的には第１の鍵生成関数から生成された鍵に加えられて共有鍵が生成される。

【００９９】

特に、第１の通信ユニット１０１は、摂動値εを生成するステップ４０７を実行するよう構成された第１の摂動値生成部２０９を含む。摂動値は、例えば、所与の確率分布内の乱数として、例えば、第１の鍵生成関数の最大可能値よりも著しく小さい最大振幅を有する一様分布等として生成され得る。

【０１００】

第１の摂動値生成部２０９及び第１の鍵生成部２０７は、第１の暗号鍵が摂動値に応じて変更されることによって第２の暗号鍵が生成されるステップ４０９を実行する第１の鍵変更部２１１に結合される。その後、第２の暗号鍵は第２の通信ユニット１０３との安全な通信のために使用される。

【０１０１】

第２の暗号鍵は特に以下のように生成され得る。

$$\widetilde{K}_{AB}=K_A(B)+\varepsilon$$

【０１０２】
図１のシステムでは、摂動値はローカルに生成され、第１の通信ユニット１０１によってのみ知られる。つまり、摂動値はＴＴＰ１０７にさえ知られず、ＴＴＰ１０７に由来する如何なる情報によってもユニークに定められない。したがって、摂動値の少なくとも一部はＴＴＰ１０７に由来する情報から決定され得ない。
【０１０３】
第１の鍵変更部２１１は、特に摂動値を（典型的にはモジュラ加算を用いて）第１の暗号鍵に加えて共有鍵を生成してもよい。したがって、ローカルキー材料及び第２の通信ユニット１０３の識別子によってユニークに決定された暗号鍵を使用せずに摂動値を使用することにより、通常はシステムに知られず、特に如何なる潜在的な攻撃者にも知られないずれ又は偏差が導入される。一例として、新たな通信が確立される度に各生成鍵に小さな乱数値が加えられることにより、通信確立の度に（場合によっては）新しい鍵が生成されてもよい。
【０１０４】
このアプローチは、共有鍵に関して第３者に不確実性を導入する。つまり、従来のシステムでは第３者は全ての共有鍵がペアワイズに対称な関数のセットから生成されると仮定することができるのに対し、図１のシステムではこれを仮定することができない。鍵は鍵生成関数を用いて生成されたものからずれている可能性がある。これは、多くの共有鍵の例が知られていたとしても、根本的な鍵生成関数の決定を著しく困難にする。つまり、結託攻撃ユニットが生成された共有鍵（すなわち、K_A（Ｃ）、K_A（Ｄ）、K_A（Ｅ）、K_A（Ｆ）等）に関する情報を共有していたとしても、付加される不確実性は、かかる鍵から根本的な関数K_A（ｘ）を決定するために要求される処理を、事実上問題を解くことができないほどに複雑にする。
【０１０５】
したがって、生成された第１の暗号鍵への付加的な摂動／ずれ／ノイズ値の付加は、結託攻撃に対する保護を大幅に向上し、実際には、多くの実践的アプリケーションにおいて結託攻撃を非現実的に又は更に事実上不可能にする。
【０１０６】
また、この例では、２つの通信ユニットによって生成された暗号鍵間の差、すなわち、共有鍵の結果と摂動値を加えていない通信ユニットにおける鍵生成関数の結果との差は、鍵生成関数間の差と加えられる摂動値によって構成される。摂動値は他方の通信ユニットには知られず、このユニットは共有鍵とローカルキーとの間の差を決定し得るが、そのいくらが摂動値に起因し、いくらが２つの鍵生成関数間の非対称性に起因するかを決定することはできない。したがって、他方の通信ユニットは、共有鍵を生成する通信ユニットの生成関数によって生成された暗号鍵をユニークに決定することができない。よって、鍵生成関数の識別子と暗号鍵との間の相関の１つのサンプルを決定することはできない。
【０１０７】
言い換えれば、攻撃通信ユニットは攻撃対象の通信ユニットのための暗号鍵をローカルに生成し、例えば、K_C（Ａ）を計算し得る。一部のシナリオでは、攻撃されている通信ユニットと更にインタラクトして共有鍵を決定し、例えば、

$$\tilde{K}_{AC}=K_A(C)+\varepsilon$$

を決定し得る。しかし、（例えば、難読値による）完全な対称性の欠如のため、K_C（Ａ）が知られたとしてもK_A（Ｃ）を知ることはできない。更に、生成された暗号鍵を合わせる処理が実行されたとしても、すなわち、例えばローカルに生成された鍵K_C（Ａ）及び共有鍵

$$\tilde{K}_{AC}$$

の両方が知られたとしても、摂動値εの不確実性はそれでもそれらからK_A（Ｃ）を決定することができないことを意味する。したがって、鍵の曖昧性除去が行われたとしても、

鍵生成関数によって生成された鍵を決定することはできない。鍵K_A（Ｃ）の不確実性は摂動値εの不確実性と同程度に大きい。

【０１０８】

複数の決定された共有鍵

$$\tilde{K}_{AC}、\tilde{K}_{AD}、\tilde{K}_{AE}、\tilde{K}_{AF}$$

から鍵生成関数を決定しようとする任意のプロセスは、共有鍵ごとに摂動値εの全ての可能な値を考慮しなければならない。これは、未知数の数を著しく増加させることによりタスクの複雑性を著しく高める。実践では、かかるアプローチは根本的な鍵生成関数を決定することを事実上不可能にする。

【０１０９】

しかし、２つの意図された機関の間で共有鍵を決定するときにも摂動値を考慮しなければならない。つまり、摂動値のため、第１の通信ユニット１０１において生成される暗号鍵、すなわちK_A（Ｂ）は、第２の通信ユニット１０３において生成される暗号鍵、すなわちK_B（Ａ）と同一ではない。したがって、暗号鍵K_B（Ａ）から共有鍵を決定するために、第２の通信ユニット１０３は演算を実行しなければならない。

【０１１０】

プロセスは、共有暗号鍵に基づいて、すなわち

$$\tilde{K}_{AC}$$

に基づいて生成されたデータを第１の通信ユニット１０１が第２の通信ユニット１０３に伝送することを含む。

【０１１１】

特に、第１の鍵変更部２１１は、第２の暗号鍵／共有暗号鍵を受け取るデータプロセッサ２１３に結合される。データプロセッサ２１３は、共有暗号鍵を用いてデータが生成されるステップ４１１を実行するよう構成される。

【０１１２】

データプロセッサ２１３は、更に、生成されたデータを受け取り、続いて第２の通信ユニット１０３にデータを伝送するステップ４１３を実行する第１の無線送受信機２０１に結合される。

【０１１３】

データ（以下、暗号データと呼ぶ）は、例えば、共有暗号鍵を用いて暗号化されたデータであり得る。他の例として、暗号データは、生成された暗号鍵、更に場合によっては第２の通信ユニット１０３によって知られる他のデータ、例えば暗号化されずに第２の通信ユニット１０３に伝送される他のデータ、第２の通信ユニット１０３から先に受信されたナンス、又は所定の且つ場合によっては標準化されたデータに基づく暗号ハッシュであり得る。

【０１１４】

第２の通信ユニット１０３は、第１の通信ユニット１０１及び本例ではＴＴＰ１０７を含む他の通信ユニットのＯＴＡインターフェイスと通信するよう構成された第２の無線送受信機３０１を含む。第２の無線送受信機３０１は第１の無線送受信機２０１と類似又は同一であり、第１の無線送受信機２０１に対して与えられるコメントは等しく第２の無線送受信機３０１に関連する。

【０１１５】

第２の通信ユニット１０３は、第２の無線送受信機３０１に結合され、ＴＴＰ１０７に由来するローカルキー材料を取得するステップ５０１を実行するよう構成された第２の鍵材料プロセッサ３０３を含む。

【０１１６】

この特定の例では、ローカルキー材料は（安全な）無線通信によってＴＴＰ１０７から

受信されるが、他の実施形態では、内部及び外部ソースの両方を含め、他のソースから取得され得ることを理解されたい。例えば、ローカルキー材料は製造中にＴＴＰ１０７によって提供され、第１の通信ユニット１０１のローカルストレージ内に記憶されてもよい。他の例として、着脱可能メモリ（例えば、メモリカード又はＵＳＢ）等の適切なポータブルメディアから提供されてもよい。

【０１１７】

ローカルキー材料は、安全な暗号オペレーションをサポートするために要求される暗号鍵を生成するために使用され得る第２の鍵生成関数K_B（ｘ）を定める。第２の鍵生成関数は第２の通信ユニット１０３に固有であり、１つ以上の通信ユニットの識別子（又は、同等に、通信ユニットに関連付けられたユーザの識別子）に基づき暗号鍵を与える。

【０１１８】

この例では、第２の鍵生成関数は、ＴＴＰ１０７によって配信されるペアワイズなほぼ対称な鍵生成関数のセットの他の関数である。したがって、この例では、第２の生成関数は第１の通信ユニット１０１に提供された第１の鍵生成関数と略対称ではあるが完全に対称ではない通信ユニット（又はユーザ）識別子の一変数関数であり、すなわち、K_A（Ｂ）　K_B（Ａ）である。

【０１１９】

この例では、ローカルキー材料は第２の鍵生成関数をユニークに定める。

【０１２０】

この特定の例では、ローカルキー材料は暗号鍵を生成するために使用される多項式を定める。

【０１２１】

したがって、ステップ５０１において、第２の鍵材料プロセッサ３０３は、第２の鍵生成関数をユニークに定めるローカルキー材料を取得する。

【０１２２】

第２の通信ユニット１０３は、更に、第１の通信ユニット１０１の識別子、すなわち、安全な通信がイニシャライズされようとしている対象の通信ユニットの識別子を第２の通信ユニット１０３が決定するステップ５０３を実行するよう構成された第２の識別子プロセッサを含む。

【０１２３】

第１の通信ユニットの識別子は任意の方法で決定され、例えば、第１の通信ユニット１０１から受信されるメッセージに応じて決定され得ることを理解されたい。

【０１２４】

第２の鍵材料プロセッサ３０３及び第２の識別子プロセッサ３０５は、第２の鍵生成関数及び決定された第１の通信ユニット１０１の識別子（識別子Ａとする）を用いて第３の暗号鍵が決定されるステップ５０５を実行するよう構成された第２の鍵生成部３０７に結合される。したがって、第２の鍵生成部３０７は、第２の鍵生成関数への入力として識別子Ａを用いて第３の鍵生成関数を計算する。すなわち、第２の鍵生成部３０７は値K_B（Ａ）を計算する。

【０１２５】

従来のシステムでは、鍵K_A（Ｂ）＝K_B（Ａ）が共有鍵として使用され、よって第３の暗号鍵が直接共有鍵として使用され得る。しかし、本例では、第１の通信ユニット１０１は摂動値によって第１の暗号鍵K_A　（Ｂ）を変更することによって共有鍵を生成し、更に、鍵生成関数は対称ではない、すなわち、K_A（Ｂ）≠K_B（Ａ）である。したがって、第２の通信ユニット１０３は続いて摂動値及び非対称性に対応する第３の暗号鍵K_B（Ａ）の変形体を決定する。

【０１２６】

特に、第２の通信ユニット１０３は、第１の通信ユニット１０１によって使用された可能性がある可能な摂動値のセットが生成されるステップ５０７を実行するよう構成された第２の摂動値生成部３０９を含む。

【０１２７】
典型的には、通信ユニットによって使用され得る可能な摂動値はシステム内に既定され得る。例えば、摂動値が最大振幅P_{max}を有する付加的な値であるように、すなわち、摂動値が区間［$-P_{max}$，P_{max}］に属するように標準化されてもよい。範囲は典型的には暗号鍵の大きさよりはるかに小さい。実際には、多くの実施形態において、P_{max}は第１及び又は第２の暗号鍵の最大可能値の１０％未満である。
【０１２８】
多くの実施形態では、可能な摂動値のセットは単純に全ての可能な値、例えば［$-P_{max}$，P_{max}］の範囲内の全ての整数からなり得る。
【０１２９】
第２の摂動値生成部３０９及び第２の鍵生成部３０７は、可能な摂動値のセット及び第３の暗号鍵K_B（Ａ）を受信する第２の鍵変更部３１１に結合される。
【０１３０】
第２の鍵変更部３１１は、可能な通信ユニット摂動値のセットが第３の暗号鍵と組み合わされて可能な暗号鍵が生成されるステップ５０９を続いて実行する。第１の通信ユニット１０１が選択された摂動値を第１の暗号鍵に適用して共有鍵を生成する際に用いるアプローチと同じアプローチが用いられる。特に、モジュラスが鍵長に対応する（特に、Ｎが鍵長のとき、2^N）モジュラ加算が実行され得る。
【０１３１】
更に、第２の鍵変更部３１１は続いて、第１の通信ユニット１０１の鍵生成関数及び第２の通信ユニット１０３の鍵生成関数によって生成された暗号鍵間の可能な非対称性を考慮する。つまり、第１の鍵生成関数と第２の鍵生成関数とは対称ではないので、得られる鍵の間には差が存在する。典型的には、この差の最大値は既知であり、第２の鍵変更部３１１は続いて可能な暗号鍵にこの可能な差を加え、より大きな可能な暗号鍵のセットを生成する。
【０１３２】
例えば、ＴＴＰ１０７が最大値Δの付加的オフセットを導入し、第１の通信ユニット１０１が最大摂動値P_{max}を導入し得る場合、第２の通信ユニット１０３は、ローカルに生成された第３の暗号鍵と共有暗号鍵との間の最大差は$2・\Delta+P_{max}$であると決定できる。したがって、可能な共有暗号鍵のセットは、範囲［$-2・\Delta+P_{max}$，$2・\Delta+P_{max}$］からの整数をローカルに生成された第３の暗号鍵に加えることによって生成された全ての鍵を含み得る。
【０１３３】
したがって、第２の鍵変更部３１１は可能な共有暗号鍵のセットを生成する。したがって、生成された暗号鍵のうちの１つが共有鍵と一致するが、どれが一致するかはわからない。
【０１３４】
第２の鍵変更部３１１は、第２の無線送受信機３０１にも結合される共有鍵プロセッサ３１３に結合される。第２の無線送受信機３０１は、第１の通信ユニット１０１によって生成された暗号データが受信されるステップ５１１を実行するよう構成される。したがって、第２の無線送受信機３０１は、第１の通信ユニット１０１が共有暗号鍵を用いて生成した暗号データを受信する。このデータは共有鍵プロセッサ３１３に供給される。
【０１３５】
共有鍵プロセッサ３１３は、可能な共有暗号鍵ごとに受信暗号データに対する暗号演算が実行されるステップ５１３を実行するよう構成される。したがって、可能な共有暗号鍵のそれぞれについて、可能な暗号鍵を用いる暗号演算が受信暗号データに適用される。暗号演算は第１の通信ユニット１０１によって実行された演算に対応する。例えば、解読等の逆演算でもよいし、又は暗号ハッシュを決定する等の同じ演算でもよい。
【０１３６】
各暗号演算の結果はその後評価され、演算の結果が有効であるか否かが決定される。特

に、データを生成するために元々使用された暗号鍵と同じ暗号鍵を用いて暗号演算が実行される場合、暗号演算は有効である。

【０１３７】

使用される特定の暗号演算及び特定の有効性基準は、その特定の実施形態及び第１の通信ユニット１０１において実行される演算に依存することを理解されたい。

【０１３８】

例えば、暗号データが暗号化されたデータである場合、共有鍵プロセッサ３１３は、各可能な暗号鍵を使用して解読演算を行う。解読が成功したか否かによって演算の有効性が鍵ごとに決定される。

【０１３９】

特に、解読が有効なデータ（例えば、正しいチェックサム、マッチングする既知の特性を有するデータ等）をもたらす場合、暗号演算は有効であると考えられ、そうでない場合は無効であると考えられる。

【０１４０】

他の例として、暗号データは共有暗号鍵を用いて生成された暗号ハッシュであり得る。可能な共有暗号鍵ごとに対応する暗号ハッシュが生成され、得られたハッシュが受信されたものと比較され得る。ハッシュがマッチする場合は暗号演算が有効であると考えられ、そうでない場合は暗号演算は無効であると考えられ得る。

【０１４１】

その後、共有鍵プロセッサ３１３は有効性基準に基づき、可能な共有暗号鍵のうちの１つを選択する。特に、共有鍵プロセッサ３１３は最高の有効性指標が認められた鍵を選択し、例えば、解読が成功した又はマッチするハッシュが得られた可能な共有暗号鍵として鍵が選択される。

【０１４２】

したがって、第２の通信ユニット１０３は続いて第１の通信ユニット１０１によって生成されたものと同じ共有暗号鍵を決定する。その後、共有暗号鍵は第１の通信ユニット１０１と第２の通信ユニット１０３との間の安全な通信のために使用され得る。

【０１４３】

このアプローチは共有暗号鍵決定の複雑さを高め得るが、摂動値の不確実性を比較的低く保つことができるので、複雑さは比較的低い。

【０１４４】

しかし、通常は比較的多数の通信ユニットを要する結託攻撃に対しては、共有鍵に導入された不確実性は大幅に増加した可能な摂動の数をもたらし、よってキャパシティを著しく高め得る。

【０１４５】

この例では、鍵生成関数は、必ずしも対称ではなくほぼ対称であることだけが保証される関数、すなわち

$$K_x(y) \quad K_y(x)$$

のセットに属し得る。

【０１４６】

例えば、ＴＴＰ１０７は、各通信ユニットに対称な関数のセットに属する関数を割り当てるときに変更を導入するよう構成されてもよい。

【０１４７】

例えば、ＴＴＰ１０７は対称な関数のセットから関数を選択してもよい。かかる関数を通信ユニットに配信する前に、ＴＴＰ１０７はその関数に摂動値／難読化値を導入し得る。特に、各関数を通信ユニットに割り当てるとき、小さな値が例えば関数に加えられる。したがって、各関数は完全に対称な関数に対してオフセットされる。

【０１４８】

共有鍵はこのずれを考慮して決定され得る。特に、可能な共有鍵のセットは、第１の通信ユニット１０１によって組み入れられ得る摂動値、及び、第１の生成関数及び第２の生成関数を生成するためにＴＴＰ１０７によって完全に対称な関数に導入され得るずれの両方を考慮して生成され得る。

【０１４９】

異なる実施形態では摂動値を生成するために異なるアプローチが用いられ得る。

【０１５０】

多くの実施形態では、摂動値は単純に新しい共有鍵セットアップが実行される度に新しい乱数値として生成されてもよい。したがって、摂動値は所与の確率分布に従って選択される乱数値として単純に生成され得る。

【０１５１】

例えば、摂動値は［$-P_{max}$，P_{max}］の範囲の一様分布から決定され得る。乱数値の使用は対称な関数からのずれの不確実性を高め、結託攻撃の実行を更に著しく困難にし得る。

【０１５２】

多くの実施形態では、分布は非ゼロ平均を有するよう選択される、例えば、乱数値は非ゼロ平均の一様分布から、例えば、［$-P_{max}+1$，$P_{max}+1$］の範囲の一様分布等から生成され得る。

【０１５３】

非ゼロ平均乱数値の使用は、多くのシナリオにおいて高められたセキュリティを提供し得る。特に、非ゼロ平均は、各攻撃通信ユニットが繰り返し新しい共有鍵交換セットアップをイニシャライズし、得られた共有鍵を平均することによって第１の通信ユニット１０１が適用した第１の鍵生成関数が生成した暗号鍵に対応する平均値を得ようとすることに対する保護を高め得る。未知の平均を有する未知の確率分布を使用することで、攻撃通信ユニットが単にかかる複数の鍵生成を平均することは不可能になる。言い換えれば、たとえ攻撃通信ユニットが第１の通信ユニット１０１と攻撃通信ユニットとの間の共有鍵の平均値を決定するために多数の鍵確立を実行したとしても、摂動値を生成する確率分布の平均値を知ることはできないので、この平均値を使用して第１の暗号鍵をユニークに決定することはできない。例えば、たとえ攻撃通信ユニットが平均共有暗号鍵を決定したとしても、平均摂動値がゼロであると知られていない限り、この平均鍵が第１の暗号鍵に対応するとみなすことはできない。

【０１５４】

したがって、より一般的には、確率分布は第１の通信ユニット１０１の秘密であり、第１の通信ユニット１０１の外部に完全には知られなくてもよい。特に、確率分布の平均が第１の通信ユニット１０１の外部に知られなくてもよい。

【０１５５】

一部の実施形態では、摂動値は第２の通信ユニット１０３の識別子に応じて生成され得る。したがって、摂動値ｐは第２の通信ユニット１０３の識別子の関数であり、すなわち以下の通りであり得る。

$$p = f(B)$$

【０１５６】

特定の一例として、初めて第２の通信ユニット１０３と共有鍵が確立されるとき、第１の通信ユニット１０１は［$-P_{max}$，P_{max}］の範囲の乱数値として摂動値を生成し得る。得られた摂動値（又は対応する共有鍵）は、第１の通信ユニット１０１内に記憶され得る。同様に、第２の通信ユニット１０３が共有暗号鍵を決定したとき、第２の通信ユニット１０３はそれをローカルに記憶する。第１の通信ユニット１０１と第２の通信ユニット１０３との間のその後の通信において、各ユニットは記憶された値を引き出して各値を使用し得る。したがって、その後の通信ステップにおいて、同じ共有鍵及び同じ摂動値

が対応して使用される。かかるアプローチは、摂動値を生成するために使用される根本的な確率分布を推定するために統計的解析が使用され得ることを防ぐことができる。

【０１５７】

しかし、このアプローチは同時にかなりの量のメモリを要し得る。他のアプローチは、摂動値を第２の通信ユニット１０３の識別子の決定論的な値として決定することであり得る。他の例として、摂動値は、第２の通信ユニット１０３の識別子から決定されたランダムシードを用いて生成される暗号ハッシュ（より一般的には、疑似ランダム関数）のｘのＬＳＢとして決定されてもよい。

【０１５８】

したがって、このシステムでは、共有鍵はＴＴＰ１０７によって定められる鍵生成関数に基づいて生成される。しかし、この鍵を直接使用する代わりに摂動値が鍵に加えられ、摂動値はＴＴＰ１０７によってユニークに決定されない。むしろ、摂動値は第１の通信ユニット１０１にしか知られない情報に少なくとも基づいて第１の通信ユニット１０１内でローカルに生成される。特に、摂動値は、ＴＴＰ１０７によって供給されるいずれの情報に関してもランダムな要素を含み得る。選択される摂動値の正確な値は第１の通信ユニット１０１の外部には知られない。

【０１５９】

上記は、第１の通信ユニット１０１が摂動値を加えることによって共有暗号鍵を生成する一方、第２の通信ユニット１０３は単にこの共有暗号鍵にローカルに生成された自身の暗号鍵を合わせる一例に焦点を当てる。しかし、多くの実施形態では、両方／全ての通信ユニットが、摂動値を加えることによって共有鍵を生成するための機能、及びローカルに生成された自身の鍵を他の通信ユニットによって生成された共有鍵に合わせる機能の両方を備え得ることを理解されたい。したがって、第１の通信ユニット１０１は更に第２の通信ユニット１０３に関して説明された機能を備えてもよく、その逆もあり得る。

【０１６０】

また、どの通信ユニットが摂動値及び共有鍵を生成するかの選択は、任意の適切なアプローチに従って決定され得ることを理解されたい。例えば、通信確立を持ちかける通信ユニットが共有暗号鍵を生成する通信ユニットであってもよい。

【０１６１】

次に、鍵共有をイニシャライズするためのアプローチの特定の一例を説明する。この例では、鍵共有は確立フェース及び使用フェーズを備える。確立フェーズは開始ステップ及び登録ステップを含み得る。開始ステップは通信ユニットに関与しない。

【０１６２】

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ものとするが、これは必須ではないことを留意されたい。

【０１６３】

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ｂ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、ｂ＝２５６以上の値が好ましい可能性がある。

【０１６４】

この例では、鍵生成関数は多項式である。

【０１６５】

多項式の望ましい次数が選択される。次数はいくつかの多項式の次数を制御する。次数

を「ａ」とする（１≦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。

【０１６６】

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。

【０１６７】

セキュリティパラメータａ及びｍの高い値は、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。

【０１６８】

一実施形態では、$2^{(a+2)^b-1} \leqq N$を満たし、最も好ましくは更に$N \leqq 2^{(a+2)^b}-1$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。

【０１６９】

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、信頼機関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。

【０１７０】

ｍ個のペアワイズに異なる秘密モジュラス$p_1, p_2, \ldots, p_m$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、$\gamma_j$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、$-2^b+1 \leqq \gamma_j \leqq 2^b-1$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。

【０１７１】

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$a_j \leqq a$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。

【０１７２】

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これらの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に対応する値γ_j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

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

という形式でも記載される（ｊ＝１，２，．．．，ｍ）。

【０１７３】

上記例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多様に選択され、特に一変数多項式を難読化するよう選択され得る。これは、互いに異なるが、十分に頻繁に十分に互いに近い多項式を生成することに基づき鍵を生成するために特に使用され得る。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、及び通信ユニット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、多項式鍵の生成時に実行されるモジュラ演算が整数に加えられるとき、非線形的に組み合わせられるよう正の整数を組み合わせ、通信ユニット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のサイズは全ての通信ユニット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。

【０１７４】

登録ステップ

登録ステップでは、各通信ユニットに鍵材料（ＫＭ）が割り当てられる。通信ユニット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。

【０１７５】

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。

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

【０１７６】

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。＜・・・＞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、係数の長さ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。鍵材料は係数c_i^Aの形式でデバイスＡ上に記憶される。

【０１７７】

したがって、この例では、ＴＴＰは完全に対称な関数に対応しないローカルキー材料を提供する。各通信ユニットの各鍵生成関数にはランダムな変更（難読化）が導入された。

この根本的な対称関数の難読化は、各通信ユニットにおいて生成される鍵を完全に同一ではなくさせ、よって結託攻撃を著しく困難にする。

【０１７８】

一変数多項式

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

の評価は、それぞれ、より小さいモジュラスｐ$_{j}$を法としたモジュロ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。実際では、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）ペアのコレクションを、好ましくはコレクション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。

【０１７９】

Ｎ及び整数ｐ$_{j}$に関するより一般的な構造が使用される場合、乱数εが係数の異なる部分に影響を及ぼすよう難読化多項式を適合しなければならない。例えば、非線形効果が通信ユニット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はずである。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。

【０１８０】

使用フェーズ

２つのデバイスＡ及びＢ（例えば、図１－５の第１の通信ユニット１０１及び第２の通信ユニット１０３に対応）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第１の暗号鍵を生成する。

$$K_{AB} = << KM^A(x)|_{x=B} >_N >_{2^b} = \ll \sum_i C_i^A B^i >_N >_{2^b}$$

【０１８１】

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の第１の暗号鍵と呼ばれる０から２^{b}－１の整数である。

【０１８２】

デバイスＡはその後、例えば最大振幅Ｐ$_{max}$の乱数値として、摂動値を生成する。その後、デバイスＡは第１の暗号鍵Ｋ$_{AB}$及び摂動値εのモジュラスＮ加算によって対応する共有鍵を生成する。したがって、以下が生成される。

$$\tilde{K}_{AB}=<K_{AB}+\varepsilon>_N$$

【０１８３】
デバイスＢについては、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の第１の暗号鍵を生成できる。すなわち、デバイスＢは以下の値を計算できる。

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

【０１８４】
二変数多項式は対称ではないので、Ａの第１の暗号鍵及びＢの第１の暗号鍵は通常等しくない。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の鍵長乗後の鍵が互いに等しい可能性があり、実際にはほとんどの場合近いような条件である。
【０１８５】
上述したように、更に、Ａは続いて摂動値を加えることによって第１の暗号鍵を変更する。上記したように、この摂動値は乱数値で有り、典型的には非常に小さく保たれる。また、摂動値の加算はモジュロＮによって実行される。したがって、得られる鍵は通信ユニットによって使用される共有暗号鍵である。
【０１８６】
Ｂは通常Ｂが生成する共有暗号鍵と同一な第１の暗号鍵を生成しないが、これらの鍵はほぼ確実に互いに近い。したがって、Ｂは共有暗号鍵の可能な値を決定して、これらの可能な鍵のそれぞれについて鍵確認を実行し得る。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の共有鍵を用いた暗号化である。
【０１８７】
Ｅ（ｍ）をＢの各可能な鍵を用いて解読することにより、Ｂは鍵のいずれかが共有鍵に等しいか否かを検証できる。等しい鍵が存在する場合、ＢはＡに状況を知らせるべく応答することを選択し得る。
【０１８８】
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。
【０１８９】
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メッセージ認証コード（message authentication code；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。
【０１９０】
図６は、ＴＴＰの一部であり得る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。鍵材料取得部が、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。

【０１９１】

ルートキー生成部は、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を提供するよう構成される多項式次数要素６１２、鍵長要素６１４、及び多項式の数要素６１６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。

【０１９２】

ルートキー生成部は、公開モジュラスＮを提供するよう構成された公開モジュラス要素６１０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、速いモジュラ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６１２及び６１４によって決定される範囲内で選択される。

【０１９３】

ルートキー生成部は、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た秘密モジュラスマネージャー６２２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。

【０１９４】

ルートキー生成部は、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た対称二変数多項式マネージャー６２４を含む。対称二変数多項式は、それぞれ、係数ランダムモジュロ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）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。

【０１９５】

秘密モジュラスは、公開モジュラスに又はから２の鍵長乗の倍数を足す又は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。

【０１９６】

図７は、ＴＴＰ内に含まれ得る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。鍵材料生成部及びローカルキー材料生成部は、合わせて、鍵共有のために通信ユニットを構成するシステムを形成する。

【０１９７】

ローカルキー材料生成部は多項式操作デバイス７４０を含む。ローカルキー材料生成部は、多項式操作デバイス７４０に公開パラメータａ、Ｎを提供するための公開材料要素７１０を含む。ローカルキー材料生成部は、多項式操作デバイス７４０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７２０を含む。要素７１０及び７２０は鍵材料生成部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に接続されるメモリ又はバスであり得る。

【０１９８】
この例では、ローカルキー材料生成部は、多項式操作デバイス７４０に難読化数「$\varepsilon_{A,i}$」を提供する難読化数生成部７６０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７６０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。
【０１９９】
ローカルキー材料生成部は、ローカルキー材料が生成されるべき識別番号を例えば通信ユニット（例えば、第１の通信ユニット１０１又は第２の通信ユニット１０３）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通信ユニットに送信するよう構成された通信ユニットマネージャー７５０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通信ユニットに送信される。
【０２００】
多項式操作デバイス７４０は、マネージャー７５０からの識別番号を各二変数多項式に代入し、それぞれをモジュロ対応する秘密モジュラスによってリダクションして、（場合によっては複数の）一変数多項式を得る。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、モジュロ公開モジュラスによってリダクションされる（係数は好適には０からＮ－１の範囲内で表され得る）。
【０２０１】
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、及び鍵長も通信ユニットに送信される。したがって、ローカルキー材料は、各通信ユニット内でローカルに決定された摂動値によってその後変更され得る第１の暗号鍵を生成できる鍵生成多項式を定める。
【０２０２】
上記はローカルキー材料によって定められる鍵生成関数が多項式であるアプリケーションに焦点を当てるが、他の実施形態では他の関数であり得ることを理解されたい。
【０２０３】
本発明は、本発明を実施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にも及ぶ。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／又は静的に若しく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。
【０２０４】
上記は、明確さのために、異なる機能回路、ユニット、及びプロセッサに関連して本発明の実施形態を説明してきたことを理解されたい。しかし、本発明を損なうことなく、異なる機能回路、ユニット、又はプロセッサ間で機能を任意に適切に分散させ得ることは明らかであろう。例えば、別々のプロセッサ又はコントローラによって実行されると説明される機能が同じプロセッサ又はコントローラによって実行されてもよい。したがって、特定の機能ユニット又は回路への言及は、厳密な論理的又は物理的構造又は組織ではなく、説明される機能を提供するための適切な手段への言及に過ぎないと考えられたい。
【０２０５】
本発明は、ハードウェア、ソフトウェア、ファームウェア、又はこれらの任意の組み合わせを含め、任意の適切な形式で実装され得る。本発明は、任意で、１つ以上のデータプ

ロセッサ及び／又はデジタル信号プロセッサ上で実行されるコンピュータソフトウェアとして少なくとも部分的に実装されてもよい。本発明の一実施形態の素子及び構成要素は、任意の適切な方法で物理的に、機能的に、及び論理的に実装され得る。実際には、機能は単一のユニット若しくは複数のユニットに実装されてもよいし、又は他の機能ユニットの一部として実装されてもよい。したがって、本発明は単一のユニットに実装されてもよいし、又は、異なるユニット、回路、及びプロセッサ間に物理的に及び機能的に分散されてもよい。

【０２０６】

本発明をいくつかの実施形態に関連して説明してきたが、本発明を本明細書に記載される特定の形態に限定することは意図しない。本発明の範囲は添付の特許請求の範囲によってのみ限定される。また、ある特徴が特定の実施形態と関連して説明されているように見えたとしても、当業者は、説明される実施形態の様々な特徴が本発明に従って組み合わせられ得ることを認識するであろう。請求項において、用語「含む（又は備える若しくは有する等）」は他の要素又はステップの存在を除外しない。

【０２０７】

また、個別に列挙されていたとしても、複数の手段、要素、回路、又は方法ステップは、例えば単一の回路、ユニット、又はプロセッサによって実装され得る。更に、個別の特徴が異なる請求項内に含まれていたとしても、これらは好適に組み合され、異なる請求項内に含まれているからといって、特徴の組み合わせが実現できない及び／又は好適ではないとは限らない。また、特徴が１つのクレームカテゴリに含まれているからと言ってこのカテゴリに限定されるとは限らず、適宜他のクレームカテゴリに等しく適用可能である。また、請求項内の特徴の順番は特徴が働かなければならない順番を示唆するものではなく、特に、方法クレームの各ステップの順番は、ステップがその順番で実行されなければならないことを示唆しない。逆に、ステップは任意の適切な順番で実行され得る。また、要素は複数を除外しない。したがって、「第１の」、「第２の」等は複数を除外しない。請求項内の参照符号は単に明瞭化のための例として設けられ、特許請求の範囲を一切制限しないと解されたい。

【図１】

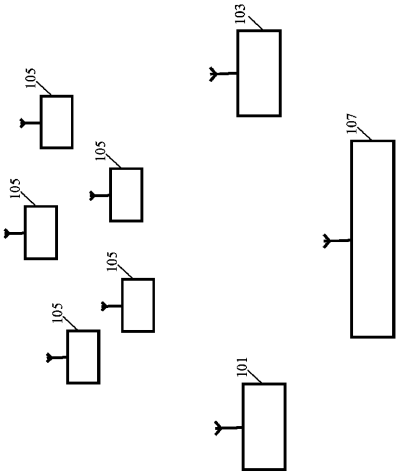


FIG. 1

【図２】

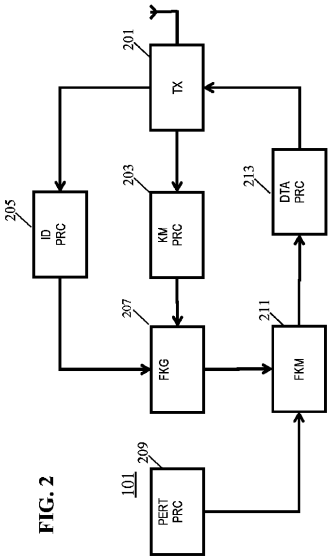


FIG. 2

【図３】

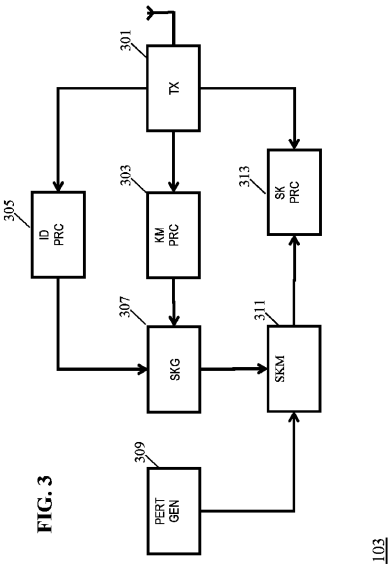


FIG. 3

【図４】

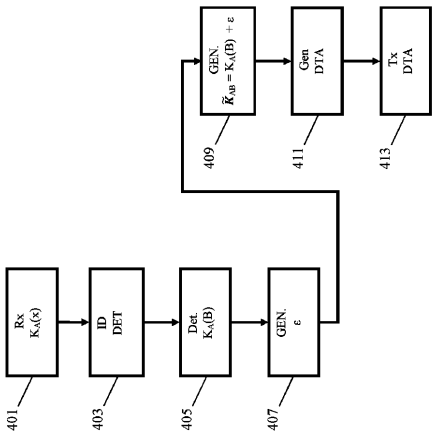


FIG. 4

【図５】

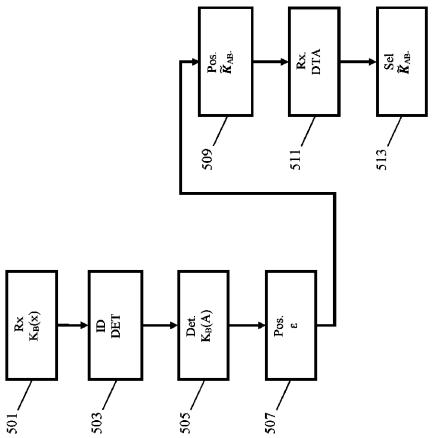


FIG. 5

【図６】

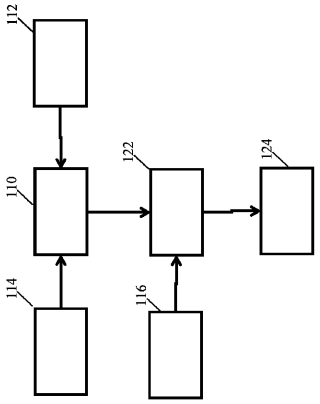


FIG. 6

【図７】

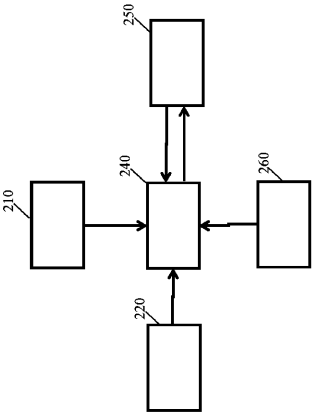


FIG. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/053224

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
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	NALIN SUBRAMANIAN ET AL: "Securing Distributed Data Storage and Retrieval in Sensor Networks", PERVASIVE COMPUTING AND COMMUNICATIONS, 2007. PERCOM '07. FIFTH A NNUAL IEEE INTERNATIONAL CONFERENCE ON, IEEE, PI, 1 March 2007 (2007-03-01), pages 191-200, XP031070401, ISBN: 978-0-7695-2787-1 section 3.3 ----- -/--	1-16

[X] Further documents are listed in the continuation of Box C. [ ] 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
28 August 2013	05/09/2013

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	Manet, Pascal

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/053224

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	Oscar Garcia Morchon, Ludo Tolhuizen, Domingo Gomez, Jaime Gutierrez: "Towards fully collusion-resistant ID-based establishment of pairwise keys", Cryptology Preprint Archive , 28 November 2012 (2012-11-28), XP055061564, Retrieved from the Internet: URL:http://eprint.iacr.org/2012/618.pdf [retrieved on 2013-04-30] cited in the application the whole document	1-16
A	WENSHENG ZHANG ET AL: "A random perturbation-based scheme for pairwise key establishment in sensor networks", PROCEEDINGS OF THE 8TH ACM INTERNATIONAL SYMPOSIUM ON MOBILE AD HOC NETWORKING AND COMPUTING , MOBIHOC '07, 9 September 2007 (2007-09-09), pages 90-99, XP055061625, New York, New York, USA DOI: 10.1145/1288107.1288120 ISBN: 978-1-59-593684-4 sections 3 and 4	1-16
A	WENSHENG ZHANG ET AL: "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks", INFOCOM 2008. THE 27TH CONFERENCE ON COMPUTER COMMUNICATIONS. IEEE, IEEE, PISCATAWAY, NJ, USA, 13 April 2008 (2008-04-13), pages 1418-1426, XP031263950, ISBN: 978-1-4244-2025-4 section III	1-16
A	MARTIN ALBRECHT ET AL: "Attacking Cryptographic Schemes Based on Perturbation Polynomials", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20090302:083331, 26 February 2009 (2009-02-26), pages 1-19, XP061003323, the whole document	1-16

-/--

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2013/053224

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHIA-MU YU ET AL: "A Simple Non-Interactive Pairwise Key Establishment Scheme in Sensor Networks", SENSOR, MESH AND AD HOC COMMUNICATIONS AND NETWORKS, 2009. SECON '09. 6TH ANNUAL IEEE COMMUNICATIONS SOCIETY CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 22 June 2009 (2009-06-22), pages 1-9, XP031493042, ISBN: 978-1-4244-2907-3 section II -----	1-16

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

Ｆターム(参考) 5J104 AA16 AA32 EA04 EA18 FA00 JA03 NA02 NA36 NA37 PA01