【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年2月15日(2018.2.15)

【公表番号】特表2016-512005(P2016-512005A)
【公表日】平成28年4月21日(2016.4.21)
【年通号数】公開・登録公報2016-024
【出願番号】特願2015-559575(P2015-559575)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｄ
Ｈ０４Ｌ　9/00　６０１Ｅ

【手続補正書】
【提出日】平成29年12月28日(2017.12.28)
【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】
第２のネットワークデバイスと共有される鍵長の共有暗号鍵を、多項式及び前記第２のネットワークデバイスの識別番号から決定する第１のネットワークデバイスであって、前記多項式は複数の項を有し、前記複数の項の各項は異なる次数及び係数と関連付けられ、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による前記多項式の評価において使用される前記多項式の表現を含む前記第１のネットワークデバイスのローカル鍵材料を保存するための電子ストレージであって、前記第１のネットワークデバイスは限られた利用可能な計算リソースを有する電子ストレージと、
前記第１のネットワークデバイスとは異なる前記第２のネットワークデバイスの前記識別番号を取得するための受信機と、
リダクションアルゴリズムに従って前記多項式を前記識別番号に適用し、前記リダクションアルゴリズムから前記共有暗号鍵を導出するためのプロセッサと
を含み、
前記リダクションアルゴリズムは、複数の繰り返しを実行することを含み、前記複数の繰り返しの各繰り返しは、前記多項式の前記複数の項にわたり実行され、前記多項式の特定の項に関連付けられた少なくとも１つの繰り返しは、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の係数の最下部との間の第１の乗算であって、前記係数の前記最下部は、前記特定の項の前記係数の鍵長の最下位ビットによって形成される、第１の乗算と、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の前記係数の更なる部分との間の第２の乗算であって、前記係数の前記更なる部分は、前記特定の項の前記係数の前記鍵長の最下位ビットとは異なるビットによって形成され、前記更なる部分及び前記最下部は、合わせて、前記多項式の前記特定の項の前記係数より厳密に少ないビットを形成し、前記更なる部分は前記特定の項の係数の最上部である、第２の乗算とを含み、
前記更なる部分のサイズは前記特定の項の次数と共に増加し、したがって、前記更なる部分の前記サイズはリダクション結果の影響が増加する場合に増加し、前記更なる部分の前記サイズは前記リダクション結果の前記影響が減少する場合に減少し、前記更なる部分

の前記増加及び前記減少の結果として、前記第１のネットワークデバイスによって利用される計算リソースに低減がある、第１のネットワークデバイス。
【請求項２】
公開モジュラスが２のべき乗＋オフセットであり、前記べき乗の指数は鍵長の倍数であり、前記オフセットの絶対値は２の鍵長乗未満であり、前記多項式の各係数は前記公開モジュラス未満である、請求項１に記載の第１のネットワークデバイス。
【請求項３】
鍵モジュラスが２の鍵長乗に等しく、前記識別番号は前記鍵モジュラス未満である、請求項１又は２に記載の第１のネットワークデバイス。
【請求項４】
前記多項式の項にわたる前記繰り返しの各繰り返しが、前記多項式の項のうちの特定の項と関連付けられ、各繰り返しは、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の係数の最下部との間の第１の乗算であって、前記係数の前記最下部は、前記特定の項の前記係数の鍵長の最下位ビットによって形成される、第１の乗算と、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の前記係数の更なる部分との間の第２の乗算であって、前記係数の前記更なる部分は、前記特定の項の前記係数の前記鍵長の最下位ビットとは異なるビットによって形成される、第２の乗算とを含む、請求項１乃至３のいずれか一項に記載の第１のネットワークデバイス。
【請求項５】
前記特定の項の前記係数の前記更なる部分は、前記特定の項の前記係数の最上部であり、前記係数の前記最上部は、前記特定の項の前記係数の複数の最上位ビットによって形成される、請求項４に記載の第１のネットワークデバイス。
【請求項６】
前記更なる部分のビット数は、鍵長の倍数である、請求項４又は５に記載の第１のネットワークデバイス。
【請求項７】
前記更なる部分のビット数は、前記特定の項の次数の減少と共に減少する、請求項４乃至６のいずれか一項に記載の第１のネットワークデバイス。
【請求項８】
前記更なる部分のビット数は、鍵長の倍数であり、前記倍数は、前記特定の項の次数＋エラー制御数に等しい、請求項７に記載の第１のネットワークデバイス。
【請求項９】
前記エラー制御数は１又は２に等しい、請求項８に記載の第１のネットワークデバイス。
【請求項１０】
前記多項式の前記係数は予備処理された形式で表現され、前記予備処理された形式において、前記特定の項の前記係数の前記最下部及び前記更なる部分は互いに隣接して単一のビット列によって表現され、前記リダクションアルゴリズムは、前記第１及び第２の乗算を合わせて実行するための前記識別番号と前記単一のビット列との間の単一の乗算を含む、請求項１乃至９のいずれか一項に記載の第１のネットワークデバイス。
【請求項１１】
第１のネットワークデバイスと第２のネットワークデバイスとの間で共有される鍵長の共有暗号鍵を、多項式及び前記第２のネットワークデバイスの識別番号から決定するための方法であって、前記多項式は複数の項を有し、前記複数の項の各項は異なる次数及び係数と関連付けられ、前記方法は、
前記第１のネットワークデバイスによる前記多項式の評価において使用される多項式の表現を含む、前記第１のネットワークデバイスのローカル鍵材料を電子形式で保存するステップであって、前記第１のネットワークデバイスは限られた利用可能な計算リソースを有するステップと、

前記第１のネットワークデバイスとは異なる前記第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、
リダクションアルゴリズムに従って前記多項式を前記識別番号に適用するステップと、
前記リダクションアルゴリズムから前記共有暗号鍵を導出するステップと
を含み、
前記リダクションアルゴリズムは、前記多項式の項にわたる繰り返しを含み、前記多項式の特定の項に関連付けられた少なくとも１つの繰り返しは、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の係数の最下部との間の第１の乗算であって、前記係数の前記最下部は、前記特定の項の前記係数の鍵長の最下位ビットによって形成される、第１の乗算と、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の前記係数の更なる部分との間の第２の乗算であって、前記係数の前記更なる部分は、前記特定の項の前記係数の前記鍵長の最下位ビットとは異なるビットによって形成され、前記更なる部分及び前記最下部は、合わせて、前記多項式の前記特定の項の前記係数より厳密に少ないビットを形成し、前記更なる部分は前記特定の項の係数の最上部である、第２の乗算とを含み、
前記更なる部分のサイズは前記特定の項の次数と共に増加し、したがって、前記更なる部分の前記サイズはリダクション結果の影響が増加する場合に増加し、前記更なる部分の前記サイズは前記リダクション結果の前記影響が減少する場合に減少し、前記更なる部分の前記増加及び前記減少の結果として、前記第１のネットワークデバイスによって利用される計算リソースに低減がある、方法。
【請求項１２】
非一時的コンピュータ可読媒体に保存された１以上の実行可能な命令を有し、プロセッサによって実行されるときに、前記プロセッサに、第１のネットワークデバイスと第２のネットワークデバイスとの間で共有される鍵長の共有暗号鍵を、多項式及び前記第２のネットワークデバイスの識別番号から決定するための方法を実行させる当該非一時的コンピュータ可読媒体であって、前記多項式は複数の項を有し、前記複数の項の各項は異なる次数及び係数と関連付けられ、前記方法は、
前記第１のネットワークデバイスによる前記多項式の評価において使用される多項式の表現を含む、前記第１のネットワークデバイスのローカル鍵材料を電子形式で保存するステップであって、前記第１のネットワークデバイスは限られた利用可能な計算リソースを有するステップと、
前記第１のネットワークデバイスとは異なる前記第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、
リダクションアルゴリズムに従って前記多項式を前記識別番号に適用するステップと、
前記リダクションアルゴリズムから前記共有暗号鍵を導出するステップと
を含み、
前記リダクションアルゴリズムは、前記多項式の項にわたる繰り返しを含み、前記多項式の特定の項に関連付けられた少なくとも１つの繰り返しは、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の係数の最下部との間の第１の乗算であって、前記係数の前記最下部は、前記特定の項の前記係数の鍵長の最下位ビットによって形成される、第１の乗算と、
前記識別番号と、前記多項式の前記表現から取得された前記特定の項の前記係数の更なる部分との間の第２の乗算であって、前記係数の前記更なる部分は、前記特定の項の前記係数の前記鍵長の最下位ビットとは異なるビットによって形成され、前記更なる部分及び前記最下部は、合わせて、前記多項式の前記特定の項の前記係数より厳密に少ないビットを形成し、前記更なる部分は前記特定の項の係数の最上部である、第２の乗算とを含み、
前記更なる部分のサイズは前記特定の項の次数と共に増加し、したがって、前記更なる部分の前記サイズはリダクション結果の影響が増加する場合に増加し、前記更なる部分の前記サイズは前記リダクション結果の前記影響が減少する場合に減少し、前記更なる部分の前記増加及び前記減少の結果として、前記第１のネットワークデバイスによって利用さ

れる計算リソースに低減がある、非一時的コンピュータ可読媒体。