

【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 6 部門第 2 区分
 【発行日】平成30年4月5日 (2018.4.5)

【公表番号】特表2018-503862(P2018-503862A)
 【公表日】平成30年2月8日 (2018.2.8)
 【年通号数】公開・登録公報2018-005
 【出願番号】特願2017-531324(P2017-531324)
 【国際特許分類】

G 0 9 C 1/00 (2006.01)

H 0 4 L 9/30 (2006.01)

G 0 6 F 21/14 (2013.01)

【F I】

G 0 9 C 1/00 6 5 0 Z

H 0 4 L 9/00 6 6 3 Z

G 0 6 F 21/14

【誤訳訂正書】

【提出日】平成30年2月22日 (2018.2.22)

【誤訳訂正 1】

【訂正対象書類名】特許請求の範囲

【訂正対象項目名】全文

【訂正方法】変更

【訂正の内容】

【特許請求の範囲】

【請求項 1】

デジタル難読化算術演算のためのパラメータを生成する電子生成装置であって、前記パラメータは有限数の環要素を有する可換環

【数 9】

$(\mathbb{Z}_n)$

を定義し、これら環要素には基底要素 (u) が、各環要素が前記基底要素の 2 つの冪の間の差分として表すことができるように含まれ、当該電子生成装置は、

素数モジュラス (p) を、該素数モジュラスが前記基底要素の所望の位数 (k) の二乗より小となる ($k^2 > p$) ように発生する素数ユニットと、

基底要素ユニットと、

を有し、該基底要素ユニットは、

1 より大きく前記素数モジュラス-1 より小さな基底要素を可能性のある基底要素 (u) として選択し、

前記可能性のある基底要素の異なる冪 ($u^0, u^1, u^2, u^3, \dots, u^{k-1}$) を発生し、

前記可能性のある基底要素 (u) が前記所望の位数と等しい位数を有するかを判定し、もし有するなら、

前記素数モジュラスのモジュロの各環要素が前記可能性のある基底要素の 2 つの冪の間の差分として表すことができるかを判定し、

前記各環要素が前記可能性のある基底要素の 2 つの冪の間の差分として表すことができると判定された場合に、前記素数及び前記基底要素を含むパラメータを生成する、電子生成装置。

【請求項 2】

前記素数ユニットが、素数（ p ）を前記所望の位数（ k ）が前記素数－1を割り切れるように発生する、請求項1に記載の電子生成装置。

【請求項3】

前記素数ユニットが、前記所望の位数の二乗より小さな全ての素数（ p ）を発生する、請求項1又は2に記載の電子生成装置。

【請求項4】

前記各環要素が前記基底要素の2つの冪の間の差分として表すことができるかについて少なくとも肯定的に判定するまで、素数及び／又は可能性のある基底要素を反復的に発生する、請求項1又は2に記載の電子生成装置。

【請求項5】

前記各環要素が前記可能性のある基底要素の2つの冪の間の差分として表すことができるかを判定する動作が、

前記素数モジュラスのモジュロの整数のリスト及び関連するフラグを発生する動作、

前記可能性のある基底要素の2つの冪の間の差分を発生すると共に、該差分に関連する前記フラグを設定する動作、及び

前記整数のリストに関連する全てのフラグが設定された場合に、前記各環要素が前記可能性のある基底要素の2つの冪の間の差分として表すことができると判定する動作、を有する、請求項1ないし4の何れか一項に記載の電子生成装置。

【請求項6】

前記リストが1から前記素数モジュラス－1までの整数からなる、請求項5に記載の電子生成装置。

【請求項7】

整数ユニットを有し、該整数ユニットが、

整数モジュラス（ n ）を、該整数モジュラスが前記基底要素の所望の位数（ k ）の二乗より小となる（ $k^2 > n$ ）ように発生し、

前記整数モジュラスの約数に対して、該約数のモジュロの各環要素が基底要素（ u' ）の2つの冪の間の差分として表すことができるような基底要素（ u' ）が存在するかを判定し、もし存在するなら、

前記整数モジュラス（ n ）のモジュロの各環要素が前記可能性のある基底要素（ u ）の2つの冪の間の差分として表すことができるかを判定する、

請求項1ないし6の何れか一項に記載の電子生成装置。

【請求項8】

可換環

【数10】

$(\mathbb{Z}_n)$

において難読化算術演算を実行する計算装置において使用するための増加テーブルを計算し、当該電子生成装置は増加テーブルを構築するテーブル生成ユニットを有し、該テーブル生成ユニットが、

入力環要素を反復して選択し、

前記入力環要素に環加算がされた増加環要素に等しい出力環要素を決定し、

前記出力環要素を符号化する出力整数リストを決定し、

前記入力環要素を前記出力整数リストにマッピングするエントリを前記増加テーブルに追加する、

請求項1ないし7の何れか一項に記載の電子生成装置。

【請求項9】

前記素数モジュラス又は整数モジュラスを発生する前に、前記所望の位数を受信するインターフェースを有する、請求項1ないし8の何れか一項に記載の電子生成装置。

【請求項10】

デジタル難読化算術演算のためのパラメータを生成するためのコンピュータの作動方法であって、前記パラメータは有限数の環要素を有する可換環を定義し、これら環要素には基底要素 (u) が、各環要素が前記基底要素の2つの冪の間の差分として表すことができるように含まれ、当該コンピュータの作動方法は、

前記コンピュータが、素数モジュラス (p) を、該素数モジュラスが前記基底要素の所望の位数 (k) の二乗より小となる ($k^2 > p$) ように発生するステップと、

前記コンピュータが、1より大きく前記素数モジュラス-1より小さな基底要素を可能性のある基底要素 (u) として選択するステップと、

前記コンピュータが、前記可能性のある基底要素の異なる冪 ($u^0, u^1, u^2, u^3, \dots, u^{k-1}$) を発生するステップと、

前記コンピュータが、前記可能性のある基底要素 (u) が前記所望の位数と等しい位数を有するかを判定するステップと、もし有するなら、

前記コンピュータが、前記素数モジュラスのモジュロの各環要素が前記可能性のある基底要素の2つの冪の間の差分として表すことができるかを判定するステップと、

前記コンピュータが、前記各環要素が前記可能性のある基底要素の2つの冪の間の差分として表すことができると判定された場合に、前記素数及び前記基底要素を含むパラメータを生成するステップと、

を有する、コンピュータの作動方法。

【請求項11】

前記コンピュータが、整数モジュラス (n) を、該整数モジュラスが前記基底要素の所望の位数 (k) の二乗より小となる ($k^2 > n$) ように発生するステップと、

前記コンピュータが、前記整数モジュラスの約数に対して、該約数のモジュロの各環要素が基底要素 (u') の2つの冪の間の差分として表すことができるような基底要素 (u') が存在するかを判定するステップと、もし存在するなら、

前記コンピュータが、前記整数モジュラス (n) のモジュロの各環要素が前記可能性のある基底要素 (u) の2つの冪の間の差分として表すことができるかを判定するステップと、

を有する、請求項10に記載のコンピュータの作動方法。

【請求項12】

コンピュータに、請求項10又は11に記載の方法の全てのステップを実行させるための、コンピュータプログラム。

【請求項13】

コンピュータ読取可能な媒体上で具現化される、請求項12に記載のコンピュータプログラム。

【誤訳訂正2】

【訂正対象書類名】明細書

【訂正対象項目名】0070

【訂正方法】変更

【訂正の内容】

【0070】

上記テーブル生成ユニットは増加テーブルを構築するように構成される。例えば、該テーブル生成ユニット140は、

入力環要素、例えば当該モジュラスのモジュロの剰余類を反復的に選択し、

入力環要素の環加算された増加環要素に等しい出力環要素を決定し、

出力環要素を符号化する出力整数リストを決定し、

入力環要素を出力整数リストにマッピングするエントリを増加テーブルに追加する、ように構成することができる。