

【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 3 区分

【発行日】令和 2 年 1 月 23 日 (2020.1.23)

【公表番号】特表 2018-538620 (P2018-538620A)

【公表日】平成 30 年 12 月 27 日 (2018.12.27)

【年通号数】公開・登録公報 2018-050

【出願番号】特願 2018-529239 (P2018-529239)

【国際特許分類】

G 0 6 F 17/10 (2006.01)

G 0 6 F 21/14 (2013.01)

【F I】

G 0 6 F 17/10 S

G 0 6 F 21/14

【手続補正書】

【提出日】令和 1 年 12 月 5 日 (2019.12.5)

【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】

主群 $(M, +)$ の 2 つの元の難読化された加算のための電子計算デバイスであって、前記主群が有限アーベル群（

【数 6 1】

$$\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$$

）であり、

前記主群に対して定義されるのは、

第 1 (N) 及び第 2 (H) の作用群であって、前記第 1 (N) 及び第 2 (H) の作用群が前記主群 (M) に作用し、前記第 2 の作用群 (H) が生成元 (h) によって生成される巡回群である ($H = \langle h \rangle$)、第 1 (N) 及び第 2 (H) の作用群と、

前記主群 (M) の第 1 の部分集合 (Δ) であって、前記主群 (M) の任意の元 (m) が、前記第 1 の作用群 (N) の元 (n) と前記第 1 の部分集合 (Δ) の元 (X) との積 ($m = nX$) として表され得る第 1 の部分集合 (Δ) において、前記第 1 の作用群 (N) の前記元 (n) と前記第 1 の部分集合 (Δ) の前記元 (X) とが、前記主群 (M) の前記元 (m) の正規化表現と呼ばれる、第 1 の部分集合 (Δ) と、

前記主群 (M) の任意の元 (m) が複数の被加数の和（

【数 6 2】

$$m = \sum_t \gamma_t m_{i_t} h^t$$

）として表され得る前記主群 (M) の第 2 の部分集合 ($M_0 = \{m_0, \dots, m_{r-1}\}$) であって、各被加数が前記第 1 の作用群 (N) の元 (γ_t) と、前記第 2 の部分集合 (M_0) の元（

【数 6 3】

$$m_{i_t}$$

）と、前記生成元の冪乗（ h^t ）との積であり、
前記複数の被加数における前記第 1 の作用群の複数の元が、前記主群（ M ）の前記元（ m ）の一般化表現と呼ばれる、第 2 の部分集合（ $M_0 = \{m_0, \dots, m_{r-1}\}$ ）と
であり、前記電子計算デバイスが、

前記第 2 の部分集合（ M_0 ）の各元（ m_i ）についてルックアップテーブル（ P_i ）を記憶する加算テーブル記憶装置であって、前記ルックアップテーブルが、前記主群（ M ）の正規化元（ (γ, X) ）を入力として取り、前記入力を前記第 1 の作用群（ N ）の元（ λ ）と前記第 1 の部分集合（ Δ ）の元（ Y ）とに写像し、前記第 1 の作用群（ N ）の前記元（ λ ）と前記第 1 の部分集合（ Δ ）の前記元（ Y ）との積が、前記正規化元（ γX ）と前記第 2 の部分集合（ M_0 ）の前記元（ m_i ）との和（ $\lambda Y h = \gamma X + m_i$ ）である、加算テーブル記憶装置と、

第 1 の加算入力（ $\alpha_0 X_0$ ）及び第 2 の加算入力（

【数 6 4】

$$\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots$$

）を受信する加算ユニットであって、前記第 1 及び第 2 の加算入力の前記主群（ M ）の元であり、前記第 1 の加算入力の前記正規化表現で受信され、前記第 2 の加算入力の前記一般化表現で受信され、前記第 1 の加算入力及び前記第 2 の加算入力の前記主群（ M ）における和を計算し、

前記第 2 の加算入力の前記被加数を前記第 1 の加算入力に順次加算することによって部分和を計算し、

前記第 2 の加算入力の被加数（

【数 6 5】

$$\gamma_t m_{i_t} h^t$$

）を前記部分和に加算することが、前記被加数における前記第 2 の部分集合（ M_0 ）の前記元（

【数 6 6】

$$m_{i_t}$$

）についての、前記加算テーブル記憶装置に記憶された前記ルックアップテーブル（

【数 6 7】

$$P_{i_t}$$

）を適用することを含む、

加算ユニットと

を備え、

$\#N \cdot \#\Delta \geq \#M$ 、及び（ $\#N \cdot \#M_0$ ） $\#H \geq \#M$ であり、ここで、

$\#N$ は第 1 の作用群（ N ）の大きさであり、

$\#H$ は第 2 の作用群（ H ）の大きさであり、

$\#\Delta$ は第 1 の部分集合（ Δ ）の大きさであり、

$\#M_0$ は第 2 の部分集合（ M_0 ）の大きさであり、

Mは主群 (M) の大きさである、
電子計算デバイス。

【請求項 2】

正規化表現の前記主群 (M) の元 (m) が、前記電子計算デバイスにおいて 2 つの数のペアとして表され、前記 2 つの数の第 1 の数が前記第 1 の作用群 (N) の前記元 (n) を示し、前記 2 つの数の第 2 の数が前記第 1 の部分集合 (Δ) の前記元 (X) を示し、

一般化表現の前記主群 (M) の元 (m) が、前記電子計算デバイスにおいて少なくとも第 1 の数の系列として表され、前記第 1 の数の系列が前記被加数における前記第 1 の作用群 (N) の前記元 (γ_t) を示す、

請求項 1 に記載の電子計算デバイス。

【請求項 3】

前記加算ユニットによって計算される前記和が正規化形式で表される、

請求項 1 又は請求項 2 に記載の電子計算デバイス。

【請求項 4】

前記電子計算デバイスの外部のコンピュータから 1 つ又は複数の加算入力を受信するネットワークインターフェースであって、前記 1 つ又は複数の加算入力一般化表現である、ネットワークインターフェースと、

1 つ又は複数の定数加算入力を正規化表現で記憶する定数記憶装置とを備え、

前記電子計算デバイスが、前記ネットワークインターフェースを介して受信される選択された加算入力と、前記定数記憶装置からの選択された定数加算入力とを前記加算ユニットを使用して加算する、

請求項 1 から請求項 3 までのいずれか一項に記載の電子計算デバイス。

【請求項 5】

変換入力を受信する変換ユニット

を備え、

前記変換入力一般化形式であり、前記変換ユニットが、正規化形式の前記主群の元を加算することによって、前記変換入力を正規化形式に変換し、及び／又は、

前記変換入力正規化入力であり、前記変換ユニットが、前記第 1 の部分集合の元を一般化形式に写像する変換テーブルを記憶する、

請求項 1 から請求項 4 までのいずれか一項に記載の電子計算デバイス。

【請求項 6】

線形関数 (f) を一般化形式の関数入力に適用する関数ユニットと、

前記第 1 の作用群 (N) の元 (γ_t) と、前記第 2 の部分集合 (M_0) の元 (

【数 6 8】

$$m_{i_t}$$

) と、前記生成元の冪乗 (h^t) との積 (

【数 6 9】

$$m = \sum_t \gamma_t m_{i_t} h^t$$

) を入力として取り、

前記積を、前記線形関数を前記積に適用した結果に写像するテーブルを記憶する線形関数テーブル記憶装置と

を備え、

前記関数ユニットが、前記線形関数テーブル記憶装置の前記テーブルを前記関数入力の前記被加数に適用する、

請求項 1 から請求項 5 までのいずれか一項に記載の電子計算デバイス。

【請求項 7】

前記第 2 の作用群 (H) が 3 つ以上の元を有するか、
 前記第 2 の作用群 (H) が 2 つの元を有するか、
 前記第 2 の部分集合 (M_0) が 2 つ以上の元を有するか、
 前記第 2 の部分集合 (M_0) が単位元でない 1 つの元を有するか、
 前記主群 (M) が、たとえば $1 \geq 4$ のアーベル群 (

【数 7 0】

$$\mathbb{Z}_2^l$$

) であるか、又は、

前記第 1 の作用群 (N) が 3 つ以上の元を有する巡回群である、
 請求項 1 から請求項 6 までのいずれか一項に記載の電子計算デバイス。

【請求項 8】

前記生成元 (h) が次数 k を有し、一般化表現の前記生成元 (h) の指数 (t) が、高々前記次数 (k) の特定の倍数マイナス 1 であり ($t \leq \lambda k - 1$)、前記特定の倍数が前記主群の全ての元について同一である、

請求項 1 から請求項 7 までのいずれか一項に記載の電子計算デバイス。

【請求項 9】

前記主群が標数 2 を有し、前記第 2 の作用群が次数 2 を有し、一般化表現の前記生成元 (h) の前記冪乗 (h^t) が、高々前記次数の 2 倍マイナス 1 であるか ($t \leq 2k - 1$)、
 又は、

前記主群が 2 より大きい標数を有するか、若しくは前記第 2 の作用群の次数が 2 より大きく、一般化表現の前記生成元 (h) の前記冪乗 (h^t) が高々前記次数マイナス 1 である ($t \leq k - 1$)、

請求項 8 に記載の電子計算デバイス。

【請求項 10】

前記加算ユニットが、
 前記部分和を最初は前記第 1 の加算入力 (α_0, X_0) に設定し、
 前記第 1 の加算入力の前記被加数にわたってループし、各ループにおいて、前記第 1 の加算入力の前記被加数 (

【数 7 1】

$$\gamma_t m_{i_t} h^t$$

) を加算することによって前記部分和を更新する、

請求項 1 から請求項 9 までのいずれか一項に記載の電子計算デバイス。

【請求項 11】

前記第 1 の加算入力 $\alpha_0 \in N$ 及び $X_0 \in \Delta$ での前記主群の元 $\alpha_0 X_0$ であり、前記第 2 の加算入力 α_1 が前記主群の元

【数 7 2】

$$\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \cdots \gamma_{\lambda k - 1} m_{i_{\lambda k - 1}} h^{\lambda k - 1}$$

であり、k が前記生成元の次数であり、 $\gamma_i \in N$ 及び $m_i \in M_0$ であり、h が前記生成元であり、

前記加算ユニットが、
 前記部分和を最初は前記第 1 の加算入力 α_0, X_0 に設定し、
 0 から $\lambda k - 1$ までの前記生成元 (h^t) の各指数 (t) について、

【数 7 3】

$$m_{i_t}$$

についての前記ルックアップテーブル（

【数 7 4】

$$P_{i_t}$$

）を $\gamma_{t-1} \gamma_{t-1} \alpha_t X_t$ に適用して、前記指数（

【数 7 5】

$$\gamma_t m_{i_t} h^t$$

）に対応する前記被加数を加算することによって、現在の部分 and（ $\alpha_t X_t$ ）から次の部分 and（ $\alpha_{t+1} X_{t+1}$ ）を取得し、 γ^{-1} が前記主群（M）の単位元であり、 $\alpha_t X_t$ が前記現在の部分 and であり、

前記部分 and が $\gamma_{t-1} \alpha_t X_t h^t$ に等しい、

請求項 10 に記載の電子計算デバイス。

【請求項 12】

前記第 1 の部分集合（ Δ ）が、前記第 1 の作用群（N）の元と、前記第 2 の部分集合の元と、前記第 2 の作用群（H）の元との積を総和して形成される元に、前記生成元の、前記生成元の次数マイナス 1 乗を加えたもの（

【数 7 6】

$$\beta_0 m_{i_0} h^0 + \cdots \beta_{k-2} m_{i_{k-2}} h^{k-2} + m_{i_{k-2}} h^{k-1})$$

）のみを含み、前記第 2 の作用群の前記元が、高々前記生成元の次数マイナス 2 乗の前記生成元（h）の冪乗である、

請求項 1 から請求項 11 までのいずれか一項に記載の電子計算デバイス。

【請求項 13】

前記主群（（M, +））が、前記主群を環（（R, +, ·））にするさらなる演算（·）を有し、

第 1 の乗算入力及び第 2 の乗算入力を受信する乗算ユニットであって、前記第 1 及び第 2 の乗算入力 が主環（R）の元であり、前記第 1 の乗算入力 が正規化表現（（ $\beta_0 h^0 + \cdots \beta_{k-2} h^{k-2} + h^{k-1}$ ） $\alpha = X \alpha$ ）で受信され、前記第 2 の乗算入力 が一般化表現（ $\gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \cdots$ ）で受信され、前記第 1 の乗算入力及び前記第 2 の乗算入力の前記環（R）における積を計算し、

前記第 1 の乗算入力と、前記第 2 の乗算入力の第 1 の被加数とから第 1 の加算入力を計算し、前記第 1 の加算入力 が正規化形式（ $X(\alpha \gamma_0)$ ）であり、

前記第 1 の乗算入力と、前記第 1 の被加数以外の前記第 2 の乗算入力の複数の被加数とから 1 つ又は複数の第 2 の加算入力を計算し、前記 1 つ又は複数の第 2 の加算入力 が一般化形式（ $X(\alpha \gamma_i) h^i = (X h^i) n'$ ）であり、

前記第 1 の加算入力と前記 1 つ又は複数の第 2 の加算入力とを前記加算ユニットを介して加算する、

乗算ユニット

を備える、

請求項 12 に記載の電子計算デバイス。

【請求項 14】

（ $\#N \cdot \#M_0$ ） $\#H \geq 3/2$ （ $\#N \cdot \#\Delta$ ）であり、

より詳細には、

$(\#N \cdot \#M_0) \#H \geq 5/2 (\#N \cdot \#\Delta)$ であり、

$\#N$ が前記第1の作用群(N)の大きさであり、

$\#H$ が前記第2の作用群(H)の大きさであり、

$\#\Delta$ が前記第1の部分集合(Δ)の大きさであり、

$\#M_0$ が前記第2の部分集合(M_0)の大きさであり、

$\#M$ が前記主群(M)の大きさである、

請求項1から請求項13までのいずれか一項に記載の電子計算デバイス。

【請求項15】

主群($(M, +)$)の2つの元を加算する電子計算デバイスで使用されるルックアップテーブルを計算するためのテーブル計算デバイスであって、前記主群が有限アーベル群
【数77】

$$\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$$

であり、

第2の部分集合(M_0)の元(m_i)についての前記ルックアップテーブルを構築するテーブル作成ユニットであって、

前記主群(M)の入力された正規化元((γ, X))を繰り返し選択し、

前記入力された正規化元(γX)と前記第2の部分集合(M_0)の前記元(m_i)との和($\lambda Yh = \gamma X + m_i$)を決定し、

第1の作用群(N)の元(λ)と、第1の部分集合(Δ)の元(Y)とを、前記第1の作用群(N)の前記元(λ)と、前記第1の部分集合(Δ)の前記元(Y)との積が前記和となるように決定し、

入力された環の元を前記第1の作用群(N)の前記元(λ)と、前記第1の部分集合(Δ)の前記元(Y)とに写像する前記ルックアップテーブルにエントリを追加する

テーブル作成ユニット

を備える、テーブル計算デバイス。

【請求項16】

主群($(M, +)$)の2つの元の難読化された加算のための電子計算方法であって、前記主群が有限アーベル群

【数78】

$$\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$$

であり、

前記主群に対して定義されるのは、

第1(N)及び第2(H)の作用群であって、前記第1(N)及び第2(H)の作用群が前記主群(M)に作用し、前記第2の作用群(H)が生成元(h)によって生成される巡回群である($H = \langle h \rangle$)、第1(N)及び第2(H)の作用群と、

前記主群(M)の第1の部分集合(Δ)であって、前記主群(M)の任意の元(m)が、前記第1の作用群(N)の元(n)と前記第1の部分集合(Δ)の元(X)との積($m = nX$)として表され得る第1の部分集合(Δ)において、前記第1の作用群(N)の前記元(n)と前記第1の部分集合(Δ)の前記元(X)とが、前記主群(M)の前記元(m)の正規化表現と呼ばれる、第1の部分集合(Δ)と、

前記主群(M)の任意の元(m)が複数の被加数の和として表され得る前記主群(M)の第2の部分集合($M_0 = \{m_0, \dots, m_{r-1}\}$)であって、各被加数が前記第1の作用群(N)の元(γ_t)と、前記第2の部分集合(M_0)の元(m_i)と、

【数 7 9】

$$m_{i_t}$$

）と、前記生成元の冪乗（ h^t ）との積（

【数 8 0】

$$m = \sum_t \gamma_t m_{i_t} h^t$$

）であり、

前記複数の被加数における前記第 1 の作用群の複数の元が、前記主群（ M ）の前記元（ m ）の一般化表現と呼ばれる、第 2 の部分集合（ $M_0 = \{m_0, \dots, m_{r-1}\}$ ）とであり、前記電子計算方法が、

前記第 2 の部分集合（ M_0 ）の各元（ m_i ）についてルックアップテーブル（ P_i ）を記憶するステップであって、前記ルックアップテーブルが、前記主群（ M ）の正規化元（ (γ, X) ）を入力として取り、前記入力を前記第 1 の作用群（ N ）の元（ λ ）と前記第 1 の部分集合（ Δ ）の元（ Y ）とに写像し、前記第 1 の作用群（ N ）の前記元（ λ ）と前記第 1 の部分集合（ Δ ）の前記元（ Y ）との積が、前記正規化元（ γX ）と前記第 2 の部分集合（ M_0 ）の前記元（ m_i ）との和（ $\lambda Y h = \gamma X + m_i$ ）である、記憶するステップと、

第 1 の加算入力（ $\alpha_0 X_0$ ）及び第 2 の加算入力（

【数 8 1】

$$\gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \gamma_2 m_{i_2} h^2 + \dots$$

）を受信し、前記第 1 及び第 2 の加算入力が前記主群（ M ）の元であり、前記第 1 の加算入力が正規化表現で受信され、前記第 2 の加算入力が一般化表現で受信され、前記第 1 の加算入力及び前記第 2 の加算入力の前記主群（ M ）における和を計算するステップであって、

前記第 2 の加算入力の前記被加数を前記第 1 の加算入力に順次加算することによって部分和を計算するステップ

を有し、

前記第 2 の加算入力の被加数（

【数 8 2】

$$\gamma_t m_{i_t} h^t$$

）を前記部分和に加算するステップが、前記被加数における前記第 2 の部分集合（ M_0 ）の前記元（

【数 8 3】

$$m_{i_t}$$

）についての、記憶された前記ルックアップテーブル（

【数 8 4】

$$P_{i_t}$$

）を適用するステップを有する、

計算するステップと

を有し、

$\# N \cdot \# \Delta \geq \# M$ 、及び $(\# N \cdot \# M_0) \# H \geq \# M$ であり、ここで、

$\# N$ は第 1 の作用群 (N) の大きさであり、

$\# H$ は第 2 の作用群 (H) の大きさであり、

$\# \Delta$ は第 1 の部分集合 (Δ) の大きさであり、

$\# M_0$ は第 2 の部分集合 (M_0) の大きさであり、

$\# M$ は主群 (M) の大きさである、

電子計算方法。

【請求項 17】

主群 ($(M, +)$) の 2 つの元を加算する電子計算デバイスで使用するルックアップテーブルを計算するためのテーブル計算方法であって、前記主群が有限アーベル群 (

【数 85】

$$\mathbb{Z}_{p_1}^{k_1} \oplus \dots \oplus \mathbb{Z}_{p_t}^{k_t}$$

) であり、

前記主群 (M) の入力された正規化元 ((γ, X)) を繰り返し選択するステップと

、

前記入力された正規化元 (γX) と第 2 の部分集合 (M_0) の前記元 (m_i) との和 ($\lambda Y h = \gamma X + m_i$) を決定するステップと、

第 1 の作用群 (N) の元 (λ) と、第 1 の部分集合 (Δ) の元 (Y) とを、前記第 1 の作用群 (N) の前記元 (λ) と、前記第 1 の部分集合 (Δ) の前記元 (Y) との積が前記和となるように決定するステップと、

入力された環の元を前記第 1 の作用群 (N) の前記元 (λ) と、前記第 1 の部分集合 (Δ) の前記元 (Y) とに写像する前記ルックアップテーブルにエントリを追加するステップと

を有する、テーブル計算方法。

【請求項 18】

コンピュータ上で実行された場合に、請求項 16 に記載の電子計算方法又は請求項 17 に記載のテーブル計算方法を実施するコンピュータプログラム命令を含む、コンピュータプログラム。

【請求項 19】

請求項 18 に記載のコンピュータプログラムを含む、コンピュータ可読媒体。