

(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2018-538620

(P2018-538620A)

(43) 公表日 平成30年12月27日(2018.12.27)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 17/10 (2006.01)	G06F 17/10	S 5B056
G06F 21/14 (2013.01)	G06F 21/14	

審査請求 未請求 予備審査請求 有 (全 47 頁)

(21) 出願番号	特願2018-529239 (P2018-529239)	(71) 出願人	590000248
(86) (22) 出願日	平成28年12月7日 (2016.12.7)		コーニンクレッカ フィリップス エヌ
(85) 翻訳文提出日	平成30年6月6日 (2018.6.6)		ヴェ
(86) 国際出願番号	PCT/EP2016/079971		KONINKLIJKE PHILIPS
(87) 国際公開番号	W02017/097791		N. V.
(87) 国際公開日	平成29年6月15日 (2017.6.15)		オランダ国 5656 アーエー アイン
(31) 優先権主張番号	2015911		ドーフエン ハイテック キャンパス 5
(32) 優先日	平成27年12月7日 (2015.12.7)		High Tech Campus 5,
(33) 優先権主張国	オランダ (NL)		NL-5656 AE Eindhoven
		(74) 代理人	110001690
			特許業務法人M&Sパートナーズ

最終頁に続く

(54) 【発明の名称】 計算デバイス及び方法

(57) 【要約】

主群 $(M, +)$ の2つの元を加算するように構成された電子計算デバイスであって、主群が有限アーベル群、式 (I) であり、— 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 110 と、— 第1の加算入力 $(\alpha_0 X_0)$ 及び第2の加算入力 $(\gamma_0 m_{i0} h^0 + \gamma_1 m_{i1} h^1 + \gamma_2 m_{i2} h^2 + \dots)$ を受信するように構成された加算ユニットであって、第1及び第2の加算入力为主群 (M) の元であり、第1の加算入力が正規化表現で受信され、第2の加算入力が一般化表現で受信され、第1の加算入力及び第2の加算入力の主群 M における和を計算する、加算ユニットとを備える、電子計算デバイス。

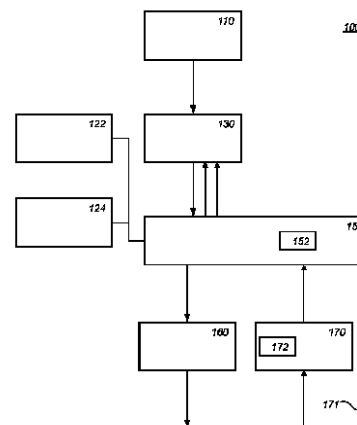


Fig. 1a

【特許請求の範囲】

【請求項 1】

主群（（M，+））の 2 つの元を加算する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 = 〈h〉）、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 = n X）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 3】

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

）として表され得る前記主群（M）の第 2 の部分集合（M₀ = {m₀, . . . , 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（M₀）の元（

【数 6 2】

$$m_{i_t}$$

）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（M₀ = {m₀, . . . , 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（M₀）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（γ X）と前記第 2 の部分集合（M₀）の前記元（m_i）との和（λ Y h = γ X + m_i）である、加算テーブル記憶装置と、

第 1 の加算入力（α₀ X₀）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 の加算入力前記主群（M）の元であり、前記第 1 の加算入力前記正規化表現で受信され、前記第 2 の加算入力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 の加算入力前記主群（M）における和を計算し、

10

20

30

40

50

前記第 2 の加算入力の前記被加数を前記第 1 の加算入力の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 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が一般化表現である、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 乃至 3 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、

前記変換入力が一般化形式であり、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、

前記変換入力が正規化入力であり、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 乃至 4 のいずれか一項に記載の電子計算デバイス。

10

20

30

40

50

【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】

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

10

）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 乃至 5 のいずれか一項に記載の電子計算デバイス。

【請求項 7】

20

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、

30

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 乃至 6 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 乃至 7 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、

40

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（

50

【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 乃至 9 のいずれか一項に記載の電子計算デバイス。

【請求項 1 1】

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、前記主群の元

【数 7 2】

10

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

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】

20

$$m_{i_t}$$

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】

30

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

）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 ($\alpha_t X_t$) から次の部分 ($\alpha_{t+1} X_{t+1}$) を取得し、 γ^{-1} が前記主群 (M) の単位元であり、 $\alpha_t X_t$ が前記現在の部分であり、

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

請求項 10 に記載の電子計算デバイス。

【請求項 1 2】

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（

40

【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 乃至 11 のいずれか一項に記載の電子計算デバイス。

【請求項 1 3】

前記主群 ($(M, +)$) が、前記主群を環 ($(R, +, \cdot)$) にするさらなる演算 ($\cdot$

50

）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の乗算入力の前記主環（ R ）の元であり、前記第1の乗算入力正規化表現（ $(\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}) \alpha = X \alpha$ ）で受信され、前記第2の乗算入力一般化表現（ $\gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \dots$ ）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乃至13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、

前記第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（ $\lambda Y h = \gamma X + m_i$ ）を決定し、

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つの元を加算する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

10

20

30

40

【数 7 8】

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

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 = (h))、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 (

【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 (

10

20

30

40

50

【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】

$$m_{i_t}$$

10

）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
を有する、電子計算方法。

【請求項 1 7】

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方法であって、前記主群が有限アーベル群（

20

【数 8 5】

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

）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（ $\lambda Y h = \gamma X + m_i$ ）を決定するステップと、

30

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 1 8】

コンピュータ上で実行された場合に、請求項 1 6 又は 1 7 に記載の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。

40

【請求項 1 9】

請求項 1 8 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。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、電子計算デバイス、電子計算方法、テーブル計算デバイス、テーブル計算方
法及びコンピュータプログラム、並びにコンピュータ可読媒体に関する。

【背景技術】

【0002】

ホワイトボックス暗号、より一般的にはソフトウェア難読化において、単純な値ではな

50

く符号化された値に対して計算が行われることが多い。単純な値そのものではなく、符号化された値に対して計算が行われる場合、難読化されたソフトウェアのリバースエンジニアリングはより困難になる。

【0003】

符号化の後では、コンピュータの組み込みのプリミティブを使用して、加算又は乗算などの通常の演算を行うことはできなくなる。符号化された値の単純な加算は、通常、値の加算の符号化とはならない。同じことが乗算にも当てはまる。公式では、ほとんどの x 及び y について、 $E(x) + E(y) \neq E(x + y)$ であり、 E は符号化関数を表す。

【0004】

この問題の解決策は、加算 (A) 及び乗算 (M) のテーブルを導入することである。これらのテーブルは2つの符号化された値を入力として取り、加算又は乗算演算の符号化に対応する符号化された値を出力として生成する。テーブルは、 $A(E(x), E(y)) = E(x + y)$ 、 $M(E(x), E(y)) = E(xy)$ として定義される。これらのテーブルは、符号化された値に対して算術が直接行われることを可能にする。

【0005】

テーブルを使用する難読化された加算及び乗算には、少なくとも2つの欠点がある。まず、テーブルが非常に大きくなり得る。 x 及び y が1ビットで表される場合、各テーブルは $2^{2^1} = 2$ ビットを必要とする。さらに、符号化は固定であり、これは攻撃者が可能な符号化のリストを作成する可能性を広げてしまう。

【発明の概要】

【発明が解決しようとする課題】

【0006】

これら及び他の懸案事項に対処する計算デバイスを有することは有利である。

【課題を解決するための手段】

【0007】

本発明者は、背景技術で論じられた、テーブルあたり約 $2^{2^1} = 2$ ビットが必要とされるものよりもはるかに小さいテーブルを使用して、加算が符号化された値に対して行われる手法を考案した。また、このシステムは、それを広く適用可能にする全てのアーベル群に適用可能である。さらに、小さいテーブル及び広い適用範囲を有することに加えて、可能性のある符号化の数は多いままであり、したがってセキュリティが向上する。

【0008】

実際に、このシステムは、冗長な変数に頼ることなく、同一の元に対する異なる表現を可能にする。これは、複数の異なる符号化が簡単に崩壊しないことを意味する。また、このシステムは、内部で使用するものとは異なる、外部データに使用される異なる符号化を可能にする（一般化表現）。また、可能な表現の数は、外部表現が二度以上使用される必要がない時点まで増加し、攻撃者が可能な符号化のリストを有効に使用する可能性をさらに低減させる。

【0009】

本発明は多数の異なる可換群 M に適用される。アーベル群としても知られている可換群は、多数の異なる馴染みのある数学的構造、たとえば、ある数を法とする整数

【数1】

$$\mathbb{Z}_n$$

又はある数及びある多項式を法とする多項式

【数2】

$$\mathbb{Z}_n[x]/f(x)$$

を含む数学的概念である。一実施形態では、このシステムは可換環に拡張される。

【0010】

本明細書でより完全に論じられるように、多数の可能性及び変形が存在する。任意の所与の実装において多数の変形のうちのいずれが選択されているかは、攻撃者には典型的には未知である。

【0011】

計算デバイスは電子デバイスであり、モバイル電子デバイス、たとえば、携帯電話、セットトップボックス、コンピュータ、スマートカードなどでもよい。

【0012】

本明細書に記載される算術は、広範囲の実際のアプリケーションに適用される。そのような実際のアプリケーションは、リバースエンジニアリングが防止されるべきである、銀行業務アプリケーションなどの、プライベートハードウェア上で動作する安全なアプリケーションを含む。他のアプリケーションは、データの不慮の漏洩が防止されるべきであるアプリケーションを含む。プログラムがプライベートデータを解放するように騙された場合、漏洩したデータが符号化されていれば、これはあまり懸念されることではない。また、算術はアプリケーションを動作させるサーバにも適用される。ユーザが符号化された形式でデータを送受信する場合、プライバシーが向上する。

【0013】

本発明による方法は、コンピュータで実施される方法として、若しくは専用ハードウェアで、又はその両方の組み合わせで、コンピュータ上に実装される。本発明による方法の実行可能コード又はその一部は、コンピュータプログラム製品に記憶される。コンピュータプログラム製品の例は、メモリデバイス、光記憶デバイス、集積回路、サーバ、オンラインソフトウェアなどを含む。好ましくは、コンピュータプログラム製品は、前記プログラム製品がコンピュータ上で実行された場合に本発明による方法を実施するためのコンピュータ可読媒体上に記憶された非一時的プログラムコード手段を含む。

【0014】

好ましい実施形態では、コンピュータプログラムは、コンピュータプログラムがコンピュータ上で実行された場合に、本発明による方法の全てのステップを実施するように適合された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、コンピュータ可読媒体上に具現化される。

【0015】

本発明のさらなる詳細、態様、及び実施形態が、図面を参照して単なる例として説明される。図中の要素は簡潔かつ明瞭にするために示されており、必ずしも縮尺通りに描かれていない。図面では、説明済みの要素に対応する要素は同一の参照番号を有する場合がある。

【図面の簡単な説明】

【0016】

【図1a】計算デバイス100の一実施形態の一例を概略的に示す図である。

【図1b】加算ユニット130の一実施形態の一例を概略的に示す図である。

【図1c】乗算ユニット140の一実施形態の一例を概略的に示す図である。

【図1d】計算デバイス100'の一実施形態の一例を概略的に示す図である。

【図2】計算デバイス101の一実施形態の一例を概略的に示す図である。

【図3】計算デバイスで使用される増分テーブルを計算するためのテーブル計算デバイス200の一実施形態の一例を概略的に示す図である。

【図4】計算方法300の一実施形態の一例を概略的に示す図である。

【図5】テーブル計算方法400の一実施形態の一例を概略的に示す図である。

【図6a】一実施形態によるコンピュータプログラムを含む書き込み可能部分を有するコンピュータ可読媒体を概略的に示す図である。

【図6b】一実施形態によるプロセッサシステムの表現を概略的に示す図である。

【発明を実施するための形態】

【0017】

本発明は多くの異なる形の実施形態が可能であるが、図面に示され、本明細書で詳細に説明されるのは1つ又は複数の特定の実施形態であって、本開示が本発明の原理の例示と見なされるべきであり、本発明を図示及び説明される特定の実施形態に限定するものではないという理解の下でのものである。

【0018】

以下では、理解のために、動作中の実施形態の要素が説明される。しかしながら、それぞれの要素が、それらによって実施されるように記載された機能を実施するように構成されることは明らかであろう。

【0019】

さらに、本発明は実施形態に限定されず、本発明は上述の、又は相異なる従属請求項に記載された各新規の特徴又は特徴の組み合わせの中にある。

【0020】

図1は電子計算デバイス100の一実施形態を概略的な形で示す。計算デバイス100は主群(M, +)の2つの元を加算するように構成される。主群は元の集合Mと、Mの元の各ペアに対して定義された、+で示される2値演算とで表される。主群は群であるための通常の数学的要件を満たす(加算は結合法則を満たし、両側単位元が存在し、群の各元は逆元を有する)。さらに、群は有限かつアーベルに制限される。後者は群がある素数 p_i 及び指数 k_i について、

【数3】

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

と表されることを示す。主群について、加算は+と表記される。群の演算を+と表記、又はその単位元を0と表記するとしても、これは計算デバイスが従来の算術の意味での加算に制限されなければならないことを意味しないことに留意されたい。たとえば、ある法を法とする加算の群は、計算デバイスが適用されるアーベル群であるが、これに制限されず、代わりに任意のアーベル群に適用される。全ての群及び集合は有限であり、空ではない。

【0021】

計算デバイス100は、群における加算を計算するように構成される。群の元は、それらを符号化することによって難読化される。計算デバイスをリバースエンジニアリングしようとする攻撃者は使用された符号化を知らないので、群の元の難読化はセキュリティにとって有益である。したがって、たとえ攻撃者が計算デバイスの内部動作を観測できたとしても、そのデバイスが何を計算しているのかが分からない。

【0022】

興味深いことに、計算デバイス100は、本特許のために名付けられた2つの異なる手法、すなわち、正規化表現及び一般化表現によって群の元を符号化する。本発明者は、そのような表現が全ての有限アーベル群に対して発見されることを見出した。さらに、群は正規化表現及び一般化表現の多数の異なる選択肢を可能にする。また、後者はセキュリティを向上させ、その理由は、1つ又は少数の符号化しか利用できないのであれば、一般的な符号化システムの知識を有する攻撃者は、全ての可能な符号化を試み、どの符号化が使用されたかを解明するためである。しかしながら、符号化の多数の選択肢が利用可能である場合、後者の攻撃ラインは実行不可能になる。

【0023】

また、正規化表現及び一般化表現の両方は、同一の元の複数の異なる表現を可能にする。特に、一般化表現は、同一の群の元の多数の異なる表現を可能にするように容易に適合される。同様に、これはセキュリティにとって有益であり、1つの可能性のある攻撃ラインは、群の表現をより従来の表現に写像する変換テーブルを作成して試みることであり、しかしながら、同一の元に対してより多数の表現が存在する場合、これはより困難である。

【0024】

正規化表現及び一般化表現は、以下で論じられるいくつかの集合に対して定義される。これらの集合の選択は、表現と、それらが加算される方式、具体的には、加算で利用されるルックアップテーブル（以下でさらに論じられる）とを決定する。

【0025】

主群に対して定義されるのは、第1の作用群N及び第2の作用群Hである。これらの群の両方が主群Mに作用する。注：Aの全てのg及びBのxについて、群Bの元 $g \cdot x$ が定義される場合、群Aは群Bに作用する。群Aの単位元はxを変化させず、また、Aの任意の g_1 及び g_2 について、 $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ である。

【0026】

第2の作用群Hは、生成元(h)によって生成される巡回群である($H = \langle h \rangle$)。両方の作用群は有限である。 h^k が単位元となるような、次数と呼ばれる、ある指数kが存在する。第1及び第2の作用群の両方は、数学的意味での群である。主群への作用群の作用は積と呼ばれる。作用群の単位元は1と呼ばれる。したがって、たとえば、 $h^k \cdot x = 1 \cdot x = x$ である。第2の作用群は、好都合な表記のために、右作用として表記されていることに留意されたい。

【0027】

第1の作用群N及び第2の作用群Hは、全ての $n \in N$ 、 $m \in M$ 、 $h \in H$ について、 $(nm)h = n(mh)$ であるという性質を有するように選択されている。

【0028】

第1及び第2の作用群は、たとえば、主群Mの自己への同型写像の集合などの、Mの自己同型群の部分群として選択される。これは、第1及び第2の群が常に選択され得ることを示している。第2の作用群は、Mの自己同型群の元hを選択し、 $H = \langle h \rangle$ 、すなわち、hにより生成される群を設定することによって選択され得る。たとえば、第1及び第2の作用群は、行列群として得られる。

【0029】

必須ではないが、実施形態では、第1の作用群は

【数4】

$$Aut_{\mathbb{Z}}(M)$$

の行列部分群Nであり、hは第1の作用群Nの生成元と可換である他の行列である。この場合、列ベクトルをMの元に使用し、標準的な行列乗算によって全ての行列を左に書くことができる。作用群及びMそれぞれについての行列及びベクトルの表記は都合が良く、たとえば作用群において計算するために、又は加算テーブルを計算するために使用されるが、この形式は、たとえば符号化された表現が利用される計算デバイス自体で利用される必要はない。

【0030】

計算デバイス100における計算は、作用群で行われる計算を必要とする。作用群が、たとえば第2の作用群と同様に巡回的である場合、これは、群の次数を法とする指数で計算することによって行われる。いずれにしても、作用群での群演算を表すためにテーブルが使用される。

【0031】

また、主群に対して定義されるのは、主群Mの第1の部分集合 Δ であって、主群Mの任意の元mが $m = nX$ として、たとえば、第1の作用群Nの元nと第1の部分集合 Δ の元Xとの積として表され得るようなものである。これの他の言い方は、第1の作用群Nの作用の下での第1の部分集合 Δ の軌道が主群と等しいということである。

【0032】

第1の作用群N及び主群Mが与えられた場合、 $N \cdot M = M$ であるので、そのような第1の部分集合 Δ は存在が保証される。たとえば、第1の部分集合は、Nによって誘導されるMにおける軌道を決定し、各軌道の少なくとも1つの元を選択することによって発見され

10

20

30

40

50

る。最小の大きさの第 1 の部分集合 Δ は、各軌道のちょうど 1 つの元を選択することによって発見される。M の 2 つの元 a 及び b は、 $na = b$ となるような N の n が存在する場合、同一軌道にある。同一軌道からより多数の元を選択することは、正規化表現の数を増加させる。

【0033】

M の任意の元 m は、 $m = nX$ となる第 1 の作用群 N の元 n と、第 1 の部分集合 Δ の元 X とのペアとして表される。後者の表現は正規化表現と呼ばれる。異なる第 1 の作用群及び／又は異なる第 1 の部分集合を選択することによって、多数の異なる正規化表現が得られる。

【0034】

内部的には、ペア (n, X) は整数のペアで表される。たとえば、元 n は、N の特定の元を符号化する整数で表される。たとえば、元 X は、第 1 の部分集合 Δ の特定の元を符号化する整数で表される。この符号化は正準である必要はない。たとえば、整数の符号化は、第 1 の作用群及び／又は第 1 の部分集合にランダムな順序を与え、第 1 の作用群及び／又は第 1 の部分集合の元をその順序におけるインデックスとして表すことによって得られる。代替的には、元 n 及び X は、従来の表現、たとえば正準表現で表される。後者の表現は、それ自体が符号化され、たとえば暗号化される。

【0035】

また、主群に対して定義されるのは、主群 M の第 2 の部分集合 $M_0 = \{m_0, \dots, m_{r-1}\}$ であって、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、各被加数が、第 1 の作用群 N の元 γ_t と、第 2 の部分集合 M_0 の元 m_{i_t} と、生成元の冪乗 h^t との積であるようなものである。たとえば、

【数 5】

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

である。一般化元は、たとえば、

【数 6】

$$m = \gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \dots + \gamma_{k-1} m_{i_{k-1}} h^{k-1}$$

と記述される。後者の場合、最大の指数は第 2 の作用群の次数、すなわち、 h の次数マイナス 1 である。より一般的には、インデックス t は $\lambda k - 1$ 、すなわち、 h の次数の倍数マイナス 1 に制限される。全ての群についてではないが、 $k - 1$ の最大指数で十分であることが多い。以下、特に明記しない限り、一般化表現が高々 $k - 1$ の h の冪乗を使用すると一般に仮定する。それにもかかわらず、たとえば、より多くの一般化表現が所望される場合、以下に与えられる例はより大きい指数に拡張される。

【0036】

M の全ての元が表されることを可能にする第 2 の部分集合 M_0 が与えられた場合、集合 nM_0h^j も有効な第 2 の部分集合であり、ここで n 及び h^j はそれぞれ第 1 及び第 2 の作用群のものである。

【0037】

一般化形式の元は 2 つの系列、すなわち、 $\{\gamma_0, \gamma_1, \dots, \gamma_{k-1}\}$ 及び

【数 7】

$$\{m_{i_0}, m_{i_1}, \dots, m_{i_{k-1}}\}$$

又は $\{i_0, i_1, \dots, i_{k-1}\}$ と表される。後者の系列は、元をリストにおけるそれらのインデックスによって表す一例である。また、元 γ_i は整数として、たとえば、N のリスト表現におけるインデックスとして表される。一実施形態では、第 2 の部分集合

10

20

30

40

50

は単一の元 m_0 を含み、この場合、第 2 の系列は明示的である必要はなく、暗黙的でもよい。一実施形態では、系列は、 M の全ての元について同一の長さを有する。一実施形態では、系列は、0 から h の限度までの、たとえば、 $k-1$ 又は $\lambda > 1$ での $\lambda k-1$ までの h の各冪乗についてのエントリを有する。

【0038】

また、2 つの系列は単一の系列、たとえば、
【数 8】

$$\{\gamma_0, m_{i_0}, \gamma_1, m_{i_1}, \dots, \gamma_{k-1}, m_{i_{k-1}}\}$$

10

と表される。

【0039】

以下の境界、 $\#N \cdot \#\Delta \geq \#M$ 、及び $(\#N \cdot \#M_0) \#^H \geq \#M$ を有し、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。

【0040】

また、第 1 の作用群 (N)、第 2 の作用群 (H)、第 1 の部分集合 (Δ)、第 2 の部分集合 (M_0)、及び主群 (M) の大きさはいずれも空ではない。所望であれば、正規化表現の数は、主群 M の大きさに比べて上限が与えられ得、たとえば、いくつかの実施形態では、 $2\#M \geq \#N \cdot \#\Delta$ である。これは、正規化元の数制限することが加算テーブルの大きさを減少させるので、利点を有する場合がある。しかしながら、これは必須ではないことに留意すべきであり、具体的には、表現の数、特に一般化表現の数が、群の大きさに比べて大きいことが望ましい場合がある。たとえば、正規化表現の数は、より大きい第 1 の作用群又はより大きい第 1 の部分集合を選択することによって増加し、一般化表現の数は、 h に対してより大きい指数を許可するか、又はより大きい作用群又はより大きい第 2 の部分集合を選択することによって増加する。

20

【0041】

図 1 はオペランド記憶装置 150 を示す。オペランド記憶装置 150 は、加算対象の群 M の元を記憶する。また、加算以外の他の演算、たとえば乗算などが、オペランド記憶装置 150 内の元に対して行われる。オペランド記憶装置 150 は、正規化表現及び一般化表現のオペランドを含む。オペランド記憶装置 150 の一部は、正規化表現の 1 つ又は複数の定数加算入力を記憶するように構成される定数記憶装置 152 である。また、オペランド記憶装置 150 は、一般化形式の定数を含む。 M の元が加算されたか、さもなければ計算された後、それらはオペランド記憶装置 150 に、たとえば作業メモリとして再び記憶され得る。

30

【0042】

計算デバイス 100 は、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 110 を備える。そのようなルックアップテーブルは、主群 M の正規化元 (γ, X) を入力として取り、入力を第 1 の作用群 N の元 λ と第 1 の部分集合 Δ の元 Y とに写像して、第 1 の作用群 N の元 λ と第 1 の部分集合 Δ の元 Y と積が、正規化元 γX と、第 2 の部分集合 M_0 の前記元 m_i との和になる、すなわち、 $\lambda Y h = \gamma X + m_i$ となるようにする。たとえば、ルックアップテーブル P_i は、 $\lambda Y h = \gamma X + m_i$ となるように $P_i(\gamma, X) = (\lambda, Y)$ を写像する。一実施形態では、元 m_i についてのルックアップテーブルは、正規化入力を正規化出力元に写像して、正規化入力プラス (群 M の) 元 m_i が、(第 2 の作用群の作用を使用して) 生成元 h の正規化出力倍と等しくなるようにする。

40

【0043】

50

ルックアップテーブルが正規化形式のMの単一の元のみを入力として取ることに留意されたい。テーブルの大きさは正規化元の数に見合っており、これはほぼM自体の大きさである。それにもかかわらず、そのようなテーブルはMの2つの元を加算するために使用される。2つの入力を取って和を計算するテーブルは、Mの大きさの二乗で増加することに留意されたい。これは、群Mの大きさが大きくなるように、たとえば512より大きく、又は1024個の元より大きくなるように選択されても、テーブルの大きさが二次的にではなくほぼ線形に増加することを意味する。

【0044】

計算デバイス100は加算ユニット130を備える。加算ユニット130は、たとえば加算ユニット130のインターフェースなどを介して第1の加算入力及び第2の加算入力を受信するように構成され、第1の加算入力及び第2の加算入力は主群Mの元である。第1の加算入力は正規化表現、たとえば、 $\alpha_0 X_0$ で受信され、ここで α_0 は第1の作用群Nのものであり、 X_0 は第1の部分集合のものである。第2の加算入力は一般化表現、たとえば、

10

【数9】

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

で受信される。加算ユニット130は、主群Mにおける第1及び第2の加算入力の和を計算するように構成される。

20

【0045】

加算ユニット130は、第2の加算入力の被加数を第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ように構成される。第2の加算入力の被加数

【数10】

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

を部分和に加算することは、前記被加数における第2の部分集合 M_0 の元

【数11】

$$m_{i_t}$$

30

についての、加算テーブル記憶装置110に記憶されたルックアップテーブル

【数12】

$$P_{i_t}$$

を適用することを含む。

【0046】

図1bは加算ユニット130の一実施形態を示す。加算ユニット130は、第1の加算入力131と第2の加算入力132とを受信する。加算ユニット130は、第2の加算入力132から得られた被加数を第1の加算入力元に反復的に加算するように構成される部分加算ユニット134を備える。たとえば、部分加算ユニット134は、第1の加算入力131に初期化された部分和133に加算する。加算は、記憶装置110からのルックアップテーブルの適用を含む。実施形態の数学的詳細が以下でさらに論じられる。

40

【0047】

たとえば、加算ユニットは、部分和131を最初は第1の加算入力 $\alpha_0 X_0$ に設定し、第1の加算入力の被加数にわたってループし、各ループにおいて、第1の加算入力

【数 1 3】

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

の被加数を加算することによって部分和を更新するように構成される。以下、加算ユニット 1 3 0 によって第 1 及び第 2 の加算入力を加算するために使用される例示的なアルゴリズムが与えられる。

【0 0 4 8】

第 1 の加算入力 1 3 1 は主群の元 (α_0, X_0) に初期化され、ここで $\alpha_0 \in N$ 及び $X_0 \in \Delta$ であり、たとえば、第 1 の加算入力 1 3 1 はペア $\{\alpha_0, X_0\}$ と表される。第 2

10

【数 1 4】

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

であり、ここで k は生成元の次数であり、 $\gamma_i \in N$ 及び $m_i \in M_0$ であり、 h は生成元である。 $\lambda = 1$ を仮定するが、以下の式は $\lambda > 1$ の場合に直接拡張されることに留意されたい。たとえば、第 2 の加算入力 1 3 2 は、系列

【数 1 5】

$$\{\gamma_0, m_{i_0}, \gamma_1, \dots, \gamma_{k-1}, m_{i_{k-1}}\}$$

20

と表される。

【0 0 4 9】

加算ユニット 1 3 0 は、加算テーブル P の 1 つを適用した結果として得られる以下の部分的な結果の系列を計算するように構成される。以下、ルックアップテーブル P_i の正規化入力及び出力は、第 1 の作用群 N の元と第 1 の部分集合 Δ の元とのペアとして表されている。

【数 1 6】

$$(\alpha_1, X_1) \leftarrow P_{i_0}(\gamma_0^{-1} \alpha_0, X_0)$$

30

$$(\alpha_2, X_2) \leftarrow P_{i_1}(\gamma_1^{-1} \gamma_0 \alpha_1, X_1)$$

$$(\alpha_3, X_3) \leftarrow P_{i_2}(\gamma_2^{-1} \gamma_1 \alpha_2, X_2)$$

...

40

$$(\alpha_k, X_k) \leftarrow P_{i_{k-1}}(\gamma_{k-1}^{-1} \gamma_{k-2} \alpha_{k-1}, X_{k-1})$$

【0 0 5 0】

たとえば、加算ユニット 1 3 0 は、部分和を最初は第 1 の加算入力 (α_0, X_0) に設定するように構成される。たとえば 0 から $\lambda k - 1$ までの生成元の各指数 t について、部分加算ユニット 1 3 4 は、冪乗

【数 1 7】

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

に対応する被加数を加算することによって、現在の部分 and (α_t, X_t) から次の部分 and (α_{t+1}, X_{t+1}) を得る。後者は、

【数 1 8】

$$m_{it}$$

についてのルックアップテーブル

【数 1 9】

$$P_{it}$$

を ($\gamma_{t-1} \gamma_{t-1} \alpha_t, X_t$) に適用することを含み、ここで γ_{t-1} は第 1 の作用群における単位元であり、(α_t, X_t) は部分 and 1 3 3 に記憶された現在の部分 and である。

【0 0 5 1】

部分 and 1 3 3 内の部分 and (α_i, X_i) は、第 1 及び第 2 の加算入力の部分 and を表す。部分 and (α_i, X_i) は前記和と同一ではないが、値 $\gamma_{t-1} \alpha_t X_t h^t$ は部分 and、たとえば、第 1 の加算入力と、第 2 の加算入力の最初の t 個の被加数との和と等しくなる。部分 and が値 $\gamma_{t-1} \alpha_t X_t h^t$ に等しくなるように部分 and を表すことは効率的であることが分かっている。これは計算の短い系列をもたらす。しかしながら、他の表現も可能であり、具体的には、部分 and は、部分 and に直接 (定数なしで) 等しい正規化元によって表され得るが、これは不必要に加算を複雑にする。部分 and は正規化表現であることに留意されたい。加算テーブルの定義及び部分 and を代入することにより、上記のアルゴリズムが実際に正しい結果を生成することが検証され得る。アルゴリズムは第 1 の作用群における計算を含むことに留意されたい。そのような計算は任意の従来の手法で、たとえば、第 1 の作用群の何らかの正準表現を使用して、又は第 1 の作用群における計算の結果を示すテーブルを記憶するなどして行われる。

【0 0 5 2】

アルゴリズムの結果、上記アルゴリズムの最終的な部分 and (α_k, X_k) について、($\gamma_{k-1} \alpha_k X_k$) が第 1 及び第 2 の加算入力の和に等しくなる。所望であれば、加算ユニット 1 3 0 は、 $\gamma_{k-1} \alpha_k$ が計算されるさらなるステップと共に構成される。ペア $\{\gamma_{k-1} \alpha_k, X_k\}$ は正規化表現での和を表す。以下、最終的な正規化出力が、第 1 の作用群の元に γ_{k-1} を乗算することによって変換されていると仮定する。しかしながら、この最後のステップは必須でないことに留意されたい。たとえば、最後の乗算は、同一の元に行われる次の演算と組み合わせられる。特に、難読化された実装では、補正の乗算を延期する際に利点がある。たとえば、最終的な部分 and は、符号化された和と見なされる。加算の最終的な正規化出力を得るためには、 γ_{k-1} も必要であり、それは攻撃者には入手できない場合がある。

【0 0 5 3】

一実施形態では、加算ユニット 1 3 0 は、入力として 2 つの元を取り、1 つは正規化表現であり、1 つは一般化表現であり、正規化表現の元を出力として生成する。一実施形態では、加算ユニット 1 3 0 は、複数の元、たとえば 3 つ以上の元を入力として取り、1 つは正規化表現であり、残りは一般化表現であり、正規化表現の和を出力として生成する。たとえば、全ての一般化元が加算されるまで、正規化元が各一般化元に加算されて、正規化元が部分 and として生成され、複数の元の最終的な和は正規化表現である。

【0 0 5 4】

上記の例示的なアルゴリズムは、正規化元に一般化 (非正規化) 元を加算する。加算は

10

20

30

40

50

正規化入力を使用する。正規化入力は、一般化されたオペランドを正規化することによって、或いは前の加算から得られる出力若しくは他の正規化関数、又は正規化定数を使用することによって得られる。

【0055】

一実施形態では、計算デバイス100への外部入力は、非正規化されるように選択される。これは値の繰り返しを回避し、一般に、正規化元よりもはるかに多くの非正規化元を有する。たとえば、一実施形態では、いくつかの非正規化元が使用され、その後は再度使用されない。

【0056】

たとえば、入力値 x 及び定数 c によって $x + c$ を計算することが望まれる場合、正規化形式で与えられた c と、非正規化形式の x とによって $c + x$ を計算する。 $d + e = c$ によって $(d + x) + e$ を計算する方がさらに良く、ここで、 d は正規化形式であり、 x 及び e は非正規化形式である。後者の形式では、計算は c の正規化値を公開せず、これは攻撃者にとって処理中に現れる値の下に隠された実際の値を知ることを困難にする。値 c 又は値 d 及び e は、オペランド記憶装置150、たとえば定数記憶装置152に記憶される。値 d はランダムに選択され、値 e は $d + e = c$ となるように選択される。

【0057】

2つの非正規化値の加算を計算する必要がある場合、一連の演算を開始することができる正規化定数（又は複数の定数）を含めることが可能である。たとえば、 $0 + x + y$ の正規化表現は、 x 及び y が両方とも一般化されていない場合、 $x + y$ の計算を置き換えることができる。定数0は正規化元として表される。2つの正規化元を加算する必要がある場合、それらのうちの1つ、たとえば第2のものを一般化表現に置き換えることが可能である。たとえば、これは、全ての $X \in \Delta$ について、 X の一般化表現を写像するテーブルなどの写像によって行われる。一実施形態では、写像は x の複数の一般化表現を含み、その結果、 X の一般化表現の選択は一意でなく、選択を難読化するためにある程度の柔軟性を提供する。

【0058】

一実施形態では、計算デバイス100は、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ように構成されるネットワークインターフェースを備える。1つ又は複数の加算入力は一般化表現であり、1つ又は複数の加算入力に加えて、他の入力も受信され、その一部は正規化表現でもよい。定数記憶装置152には、1つ又は複数の定数加算入力が正規化表現で記憶される。計算デバイス100は、ネットワークインターフェースを介して受信された一般化形式の選択された加算入力と、定数記憶装置152からの正規化形式の選択された定数加算入力とを加算ユニットを使用して加算するように構成される。一般に、計算デバイス100は、オペランド記憶装置150内のどのオペランドに対して、加算などのどの演算が行われるかを制御するように構成される計算コントローラを備える。計算コントローラは別途図示されていない。一実施形態では、定数記憶装置は、 d が正規化され、 e が一般化されたペア (d, e) を含み、定数 d が選択された加算入力に最初に加算され、続いて定数 e が加算される。得られた正規化元は、オペランド記憶装置150に記憶される。

【0059】

正規化表現よりさらに多数の一般化表現が存在するように計算システムを構成することは比較的容易である。デバイスの外部でより多数の選択肢を有することは、外部の通信におけるセキュリティを向上させる。たとえば、一実施形態では、複数のセンサ（又は他のデバイス）が、一般化表現で符号化されたセンサデータ（又は他のデータ）を通信する。各センサは全ての一般化表現のプライベートな部分集合へのアクセスを有し、たとえば、前記複数のプライベートな部分集合のうちの2つが、たとえば、前記2つのプライベートな部分集合のいずれかの大きさの10%未満である元の閾値を超えて重複することはない。一実施形態では、前記複数のプライベートな部分集合のうちの2つが重複することはない。これは、2つのセンサが異なる表現を使用してそれらのデータを通信するという利点

10

20

30

40

50

を有する。センサへのアクセスを有し、センサデータとその一般化表現との関係をどうにかして発見した攻撃者は、この写像を使用して、異なるセンサから傍受された通信を復号することはできない。複数の、さらには多数の一般化表現を作成することがより簡単であっても、任意の所与の群の元は、複数の正規化表現によって表されてもよいことに留意されたい。

【0060】

一実施形態では、計算デバイス100は、変換入力を受信するように構成される変換ユニット150を備える。

【0061】

たとえば、変換入力是一般化形式であり、正規化形式に変換される。この場合、変換ユニット150は、正規化形式の主群の元を加算することによって、変換入力を正規化形式に変換するように構成される。その元は0でもよい。変換ユニット150は非ゼロの元を加算してもよく、その場合、たとえば符号化として入力に変更されるように、後の演算が適合される。変換ユニット150は、和が0になる複数の元であって、そのうちの少なくとも1つが正規化形式であるものを加算してもよい。

【0062】

たとえば、変換入力正規化形式であり、一般化形式に変換される。この場合、変換ユニット150は、少なくとも第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ように構成される。たとえば、写像に従って、正規化形式 $n \times X$ の X が

【数20】

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

に写像される場合、正規化形式 $n \times X$ は

【数21】

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

に写像する。 X を表す系列を $n \times X$ を表す系列に変換することは、第1の作用群において計算することによって行われる。

【0063】

変換ユニットは、表現にかかわらず主群の2つの元を加算を可能にする。たとえば、2つの元が共に正規表現である場合、そのうちの1つが一般化表現に変換される。たとえば、2つの元が共に一般化表現である場合、そのうちの1つが正規表現に変換される。

【0064】

計算デバイス100の一実施形態は関数ユニット124を備える。関数ユニットは、線形関数 f を一般化形式の関数入力に適用するように構成される。たとえば、一般化形式はオペランド記憶装置150から受信される。

【0065】

関数入力は、第1の作用群 N の元 γ_t と、第2の部分集合 M_0 の元

【数22】

$$m_{i_t}$$

と、生成元の冪乗 h^t との積

【数23】

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

を入力として取り、積を、線形関数を積に適用した結果に写像するテーブルが記憶される線形関数テーブル記憶装置を備える。関数ユニットは、線形関数テーブル記憶装置のテーブルを関数入力の被加数に適用するように構成される。たとえば、入力

【数 2 4】

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

は出力

【数 2 5】

$$f(\gamma_0 m_{i_0} h^0) + \cdots + f(\gamma_{\lambda k-1} m_{i_{\lambda k-1}} h^{\lambda k-1})$$

に写像される。一般化表現での可能な被加数の数は、一般化表現の数よりはるかに少ないことに留意されたい。したがって、線形関数 f を計算するために必要とされるテーブルは、任意の一般化元を入力として取るテーブルに必要とされるよりもはるかに小さい。非線形演算が主群 M の元の実行されてもよく、たとえばテーブルによって実行される。

【0066】

本明細書で説明された原理は、広範なアーベル群に適用可能であり、多数の表現を可能にする。以下、これらの多数の可能性の中のいくつかの選択肢が与えられる。本発明者によって行われた広範な実験は、これらの選択肢の全てについて、多数の可能な主群 M が可能であることを示している。

【0067】

一実施形態では、 h の次数が制限される。たとえば、一実施形態では、第 2 の作用群 H は 3 つの元を有するか、又は第 2 の作用群 H は 2 つの元を有する。より一般的には、次数は 4 若しくは 8 又は 16 未満などである。組み合わせて、一般化表現における指数の上限は、 $k-1$ となるように取られる。加算中に取りられるステップの数は、 H の大きさと共に増加する。たとえば、2 つ又は 3 つの元を有する比較的小さい H を選択することにより、加算はより少ないステップを有し、計算はより高速になる。

【0068】

一実施形態では、第 2 の部分集合 M_0 は少なくとも 2 つの元を有する。第 2 の部分集合の元の数を増加させることは、一般化表現の数を増加させる。具体的には、一般化表現の数は、任意の一般化表現が一度しか使用される必要がない時点まで増加する。後者は、一般化表現から変換テーブルを簡単に構成することに基づく攻撃を完全に排除する。

【0069】

一実施形態では、第 2 の部分集合の元の数が増加される。第 2 の部分集合の大きさが増加するにつれて、加算記憶装置 110 内のテーブルの数も増加する。たとえば、第 2 の部分集合の元の数、4 若しくは 8 又は 16 未満などである。具体的には、第 2 の部分集合の元数は 1 でもよい。一実施形態では、第 2 の部分集合 M_0 は、単位元でない 1 つの元を有する。

【0070】

上記のオプションは組み合わせられる。たとえば、一実施形態では、第 2 の部分集合は単一の元のみを有し、第 2 の作用群はちょうど 2 つの元を有する。十分に大きい第 1 の作用群を選択することにより、 M の全ての元が依然として表現される。

【0071】

実装に都合が良いのは、 N が巡回群、たとえば少なくとも 3 つの元を有する巡回群である選択肢である。この場合、 N はいくつかの元によって生成され、 N の元は生成元の指数として表される。指数は符号化された形式で記憶される。有利なことに、生成元は秘密に保たれ得る。

【0072】

アーベル群 M は法 n を法とする整数の群

【数 2 6】

$$\mathbb{Z}_n$$

である。剰余数系においてこれらの群の倍数を組み合わせるにより、任意の大きい数に対して算術が行われる。有利には、これらの群において指数を表す数は、実施形態の 1 つ又は複数に従って表され、再帰的定義を生成する。法 n は、たとえば 8 より大きい。

【0 0 7 3】

また、アーベル群 M は、たとえば、 $1 \geq 4$ のアーベル群

【数 2 7】

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

であり、 2^l 個の元を有することは（群

【数 2 8】

$$\mathbb{Z}_{2^l}$$

と混同されるべきでない）、2 値計算、特に XOR 演算に特に適している。

【0 0 7 4】

上記の群は標数 2 を有する。これは小さい第 2 の作用群 H 、特に 2 つの元を有する第 2 の作用群 H と組み合わせられ得る。たとえば、 H は元 $h = -1$ によって生成される。この場合、十分な一般化元を得るためには、一般化表現の生成元の冪乗 h^t は、次数マイナス $(k-1)$ を超えることが許される必要がある。一実施形態では、一般化表現における指数は、高々次数の 2 倍マイナス 1 であり、たとえば、 $t \leq 2k-1$ である。

【0 0 7 5】

主群 M が 2 より大きい標数を有するか、又は第 2 の作用群の次数が 2 より大きい場合、一般化表現の h の指数は、高々次数マイナス 1 に制限され、たとえば、 $t \leq k-1$ である。有利なことに、生成元は秘密に保たれ得、テーブルは比較的小さい。一般化元の数、たとえば、より大きい H 、 M_0 などを選択することによって、所望の大きさとなる。

【0 0 7 6】

いくつかの実施形態では、たとえば、外部入力を保護するために一般化元が使用される場合、正規化元より多数の一般化元が存在することが望ましい。これは、十分に大きい第 2 の作用群、許容可能な指数、第 2 の部分集合、さらには第 1 の作用群を選択することによって得られる。一実施形態では、 $(\#N \cdot \#M_0)^{\#H} \geq 3/2 \#N \cdot \#\Delta$ であり、すなわち、一般化表現の数は、正規化表現の数の少なくとも $3/2$ であり、より詳細には、 $(\#N \cdot \#M_0)^{\#H} \geq 5/2 \#N \cdot \#\Delta$ などである。

【0 0 7 7】

上記で論じられたように、第 1 の部分集合 Δ の元は、第 1 の作用群によって主群 M に誘導される軌道から選択される。一実施形態では、第 1 の部分集合 Δ の元は、第 1 及び第 2 の作用群並びに第 2 の部分集合から得られ、すなわち、第 1 の作用群 N の元と、第 2 の部分集合の元と、第 2 の作用群 H の元との積を総和して形成される元に、生成元の、生成元の次数マイナス 1 乗を加えたものである。第 2 の作用群の元は、高々生成元の次数マイナス 2 乗の生成元 h の冪乗である。すなわち、第 1 の部分集合 Δ の元が、

【数 2 9】

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

となるように選択され、 β_i は第 1 の作用群から取得され、 m は第 2 の部分集合から取得される。これは、機能する第 1 の部分集合を以下のように生成することが分かる：任意の

10

20

30

40

50

元が

【数 3 0】

$$m = \gamma_0 m_{i_0} h^0 + \gamma_1 m_{i_1} h^1 + \cdots + \gamma_{k-1} m_{i_{k-1}} h^{k-1}$$

と記述され得るので、後者は

【数 3 1】

$$\gamma_{k-1} (\gamma_{k-1}^{-1} \gamma_0 m_{i_0} h^0 + \cdots + \gamma_{k-1}^{-1} \gamma_{k-1} m_{i_{k-1}} h^{k-1})$$

10

と記述され、これは第 1 の作用群の元 (γ_{k-1}) と、上記で定義された第 1 の部分集合の元との積である。典型的には、第 1 の部分集合には他の多数の可能な選択肢があり、そのうちのいくつかはこの例よりも小さくてもよいことに留意されたい。しかしながら、これは、第 2 の部分集合が与えられた場合、少なくともこのようにして適切な第 1 の部分集合が構成されることを示す。

【0 0 7 8】

第 1 の部分集合の上記の構成は、第 2 の部分集合 M_0 が単一の元からなる状況にも適している。この場合、元 $\beta_0 m_0 h^0 + \cdots + \beta_{k-2} m_0 h^{k-2} + m_0 h^{k-1}$ を取得し、第 1 の部分集合の大きさの大幅な削減を与える。一般に、小さい第 1 の部分集合を有することは、正規化表現の数を減少させ、これは加算テーブルの大きさを削減する。加算

20

【0 0 7 9】

以下、主群、作用群、及び部分集合のいくつかの例が与えられる。

【0 0 8 0】

第 1 の例では、主群は群

【数 3 2】

$$M = \mathbb{Z}_3 \times \mathbb{Z}_3$$

30

である。M の元は、2 つの要素の列ベクトルとして表され得る。第 1 の作用群 N は行列

【数 3 3】

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

によって生成され、大きさ 4 を有する。第 2 の作用群は元 -1 によって生成され、 $H = \langle -1 \rangle$ であり、大きさ 2 を有する。群 H の元は $+I$ 及び $-I$ と表され、 I は単位行列を表す。第 2 の部分集合は、単一の元

40

【数 3 4】

$$m_0 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

を有する集合として選択される。M の全ての元は一般化表現で $\gamma_0 m_0 - \gamma_1 m_0$ と記述され、ここで γ_0 及び γ_1 は N のものである。第 1 の部分集合は、上記の構成を使用して集合 $\{x m_0 - m_0\}$ として選択され、ここで x は N の全ての元に及ぶ。主群、第 1 及び第 2 の作用群、並びに第 1 及び第 2 の部分集合の元は、行列又はベクトルとして表され得るが、一般的に可能であるように、何らかの符号化された形式で、たとえば、対応する群

50

又は集合のランダムな順序のインデックスとして表されてもよい。

【0 0 8 1】

第 2 の例では、主群は

【数 3 5】

$$M = \mathbb{Z}_3^4$$

である。第 1 の作用群は行列

【数 3 6】

$$\begin{bmatrix} 0 & 2 & 2 & 0 \\ 2 & 1 & 1 & 2 \\ 2 & 2 & 2 & 0 \\ 2 & 0 & 1 & 2 \end{bmatrix}$$

10

によって生成され、次数 5 を有する。第 2 の作用群は、元 -1 によって生成され、大きさ 2 を有する。第 1 の部分集合は 3 つの元を有する。

【数 3 7】

20

$$M_0 = \left\{ \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 2 \end{bmatrix} \right\}$$

第 1 の部分集合は、群 M における N の軌道の任意の元を取ることによって選択される。第 1 の部分集合は 1 7 個の元を有する。

30

【0 0 8 2】

第 3 の例では、主群は

【数 3 8】

$$M = \mathbb{Z}_2^6$$

であり、標数 2 の群である。第 1 の作用群 N は 1 4 個の元を有し、

【数 3 9】

$$g = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

40

及び、

50

【数 4 0】

$$s = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

10

によって生成される。

【0 0 8 3】

元 g は次数 7 を有し、元 s は次数 2 を有し、互いに可換である。 g 及び s によって生成される第 1 の作用群 N は次数 14 を有する。 N の全ての元は $g^i s^j$ と記述され得、整数のペア (i, j) は第 1 の作用群の元を表すために使用され得る。第 2 の部分集合は単一の元

【数 4 1】

$$m_0 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

20

30

からなる。

【0 0 8 4】

第 2 の作用群は、単位元のみを有する大きさ 1 の群である。生成元の次数 k は 1 である。この場合、一般化表現における指数の上限は、 $k - 1$ から $2k - 1$ まで増加し、したがって、2 つの被加数を有する。第 1 の部分集合は、 M 上の N の軌道から選択され、最小限の選択肢では 9 つの元を有する。

【0 0 8 5】

第 4 の例では、主群は

【数 4 2】

$$M = \mathbb{Z}_2^4$$

40

である。第 1 及び第 2 の作用群の両方は

【数 4 3】

$$\mathbb{Z}_3$$

に同形である。第 1 の作用群は

【数 4 4】

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

によって生成され、第 2 の作用群は

10

【数 4 5】

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

によって生成され、両方の生成元は次数 3 を有する。第 2 の部分集合は単一の元

20

【数 4 6】

$$m_0 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

を有する。

【0 0 8 6】

30

第 1 の部分集合は、M に誘導される N の軌道から 6 つの元が選択され得る。

【0 0 8 7】

第 5 の例では、主群は

【数 4 7】

$$M = \mathbb{Z}_4^2$$

である。第 1 の作用群は 6 つの元を有し、

【数 4 8】

40

$$\begin{bmatrix} 3 & 3 \\ 1 & 2 \end{bmatrix}$$

によって生成され、第 2 の作用群は 2 つの元を有し、

【数 4 9】

$$\begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$$

50

によって生成される。第 2 の部分集合は単一の元

【数 5 0】

$$\begin{bmatrix} 2 \\ 3 \end{bmatrix}$$

を有する。第 1 の部分集合は軌道から選択され得、5 つの元を含む。

【0 0 8 8】

例全体にわたって、第 2 の作用群の大きさは、より多くの一般化表現を作成するために増加されてもよい。同様に、第 1 及び第 2 の部分集合の大きさは増加されてもよい。加算
10 テーブルは定義式から計算され得る。

【0 0 8 9】

一般に、アーベル群 M が与えられた場合、他の元は以下のように選択される。群 M は
【数 5 1】

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$$

の積として、 $d_1 \mid d_2 \cdots \mid d_t$ によって記述される。これは、

【数 5 2】

$$M^+ = (\mathbb{Z}_{d_t})^t$$

20

の元を見つけて M に投影すれば十分であることを意味する。以下の手順に従ってもよい。

【0 0 9 0】

1. M^+ の自己同型群の生成元、たとえば、行列群

【数 5 3】

$$Mat_{t \times t}(\mathbb{Z}_{d_t})$$

の可逆元を取得する。

30

【0 0 9 1】

2. 自己同型群の元 h を、たとえば生成元のランダムな積として選択する。 h によって生成される群として H が得られる。

【0 0 9 2】

3. 自己同型群の部分群として群 N を選択する。たとえば、自己同型群において 1 つ、2 つ又はそれ以上の生成元を選択する。生成元は群 H と可換になるように選択される。 N についてそのような生成元を見つけることは、行列として見た場合に生成元の元に関する線形連立方程式を解くことによって行われることに留意されたい。

【0 0 9 3】

4. 最後に、第 1 及び第 2 の集合 M_0 及び Δ を選択する。後者は、 N の軌道を計算する
40 ことから得られる。前者は、たとえば、空集合を徐々に拡大することによって選択される。

【0 0 9 4】

最後に、このようにして得られた算術が、たとえば、 H の大きさ、一般化表現の数などの制約を満たすか否かが判定され、満たさなければ、たとえば処理はステップ 2 から繰り返される。異なるアルゴリズムが可能であり、たとえば、ステップ 2 及び 3 を入れ替えてもよいことに留意されたい。これらの構成は、たとえば効率的なメモリ使用を可能にする。

【0 0 9 5】

図 1 は、計算デバイス 100 において入力を受信するための 2 つのオプションを示す。

50

計算デバイス100は、符号化されていない入力、たとえば任意の従来の形式の主群Mの元を受信するように構成される符号化ユニット170を備える。符号化ユニット170は、入力を正規表現又は一般化表現に変換する。一実施形態では、符号化ユニット170は、群Mの元を正規表現又は一般化表現に写像するための符号化テーブルを含む。一実施形態では、符号化ユニット170は、一般化元を生成する。符号化ユニット170は計算デバイス100の一部である必要はなく、たとえば、計算デバイスは符号化された形式で、具体的には一般化表現で入力を直接受信する。たとえば、後者は、直接入力171がそこから受信される外部コンピュータに符号化ユニット170を有することによって実現される。

【0096】

一実施形態では、複数の符号化ユニット170が同一の計算デバイス100に対して生成される。複数の符号化ユニット170は、符号化されていない入力を受信し、入力を一般化表現に変換するように構成される。複数の符号化ユニット170は異なる一般化表現を使用する。たとえば、複数の符号化ユニットのうちの任意の2つの符号化ユニットに対して、主群Mの元xであって、xがその2つの符号化ユニットによって異なって符号化されるようなものが存在する。たとえば、一実施形態では、複数の符号化ユニットのそれぞれによって異なって符号化される主群Mの元xが存在する。

【0097】

また、計算デバイス100の出力は、復号ユニット160によって復号される。代替的には、計算デバイス100の出力は、符号化された形式、たとえば正規化表現又は一般化表現で返される。ローカルに、外部のコンピュータにおいて、符号化は復号ユニット160などによって取り除かれる。したがって、ユニット160及び170は共にデバイス100から省略されてもよい。

【0098】

図1dは、乗算ユニット140を含む計算デバイス100'の改良を概略的な形で示す。計算デバイス100'は、以下に示される以外は、計算デバイス100と同一である。

【0099】

この場合、主群(M, +)は環(R, +, ·)でもあり、加算に加えて、乗算も定義される。乗算は結合法則を満たし、アーベル群の演算において分配法則を満たし、単位元を有する。乗算の単位元は1と記述されることが多い。

【0100】

表記の都合上、このセクションでは、第1の作用群の作用には右表記が使用される。これは正規化元が $X\alpha$ と記述されることを意味し、ここでXは第1の部分集合のものであり、 α は第1の作用群のものである。第1及び第2の作用群は、たとえば、主環Mの自己への環同型写像の集合など、環としてMの自己同型群から取得される。

【0101】

乗算ユニット140は、第1の乗算入力141及び第2の乗算入力142を受信するように構成される。図1cは乗算ユニット140の可能な実施形態を概略的な形で与える。第1の乗算入力141及び第2の乗算入力142は主群(R)の元であり、これはこの場合、実際には環である。第1の乗算入力141は正規化表現 $X\alpha$ で受信され、第2の乗算入力142は一般化表現で受信される。乗算ユニット140は、第1の乗算入力141及び第2の乗算入力142の環(R)における積を計算するように構成される。

【0102】

乗算ユニット140は、

- 第1の乗算入力141と、第2の乗算入力142の第1の被加数とから第1の加算入力145を計算し、第1の加算入力145が正規化形式であり、
- 第1の乗算入力と、第1の加算入力145を計算するために使用された第1の被加数以外の第2の乗算入力142の複数の被加数とから1つ又は複数の第2の加算入力146を計算するように構成される。1つ又は複数の第2の加算入力146は一般化形式である。

【0103】

乗算ユニット140は、図1cに示されるように、第1の乗算入力141及び第2の乗算入力142から第1の加算入力145及び1つ又は複数の第2の加算入力146を計算するように構成される中間乗算ユニット144を備える。加算入力を決定することは、第1及び第2の作用群における演算を含むが、加算テーブルを必要としない。乗算入力から加算入力への変換の後、第1の加算入力145及び1つ又は複数の第2の加算入力146は、たとえば加算ユニット130を介して加算される。

【0104】

同一のテーブルが加算及び乗算に使用されるので、加算又は乗算のいずれが行われているかをリバースエンジニアリング中に見極めることは困難である。攻撃者が使用されるテーブルを発見できたとしても、どうにかしてその関数が加算テーブルであると把握できたとしても、加算演算又は乗算演算のいずれが行われているかはまだ分からない。さらに、乗算のために追加のテーブルが必要とされないので、コードサイズが縮小される。

【0105】

一実施形態では、第1の作用群N及び第2の作用群Hは環U(R)の単元群の部分群であり、乗算によって主群に作用し、第2の部分集合 M_0 は主群の単位元、たとえば、元 $m_0 = 1$ のみを含む。この場合、第1の部分集合は、上述されたように、元 $\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}$ として構成される。この場合、第1の乗算入力141は、 $(\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}) \alpha = X \alpha$ の形を有し、第2の乗算入力142は、 $(\gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \dots)$ の形を有する。

【0106】

以下、乗算入力を加算入力に変換する変換アルゴリズムの一例が与えられる。第1の乗算入力141を $r = X \alpha = (\beta_0 h^0 + \dots + \beta_{k-2} h^{k-2} + h^{k-1}) \alpha$ とし、第2の乗算入力142を $r' = \gamma_0 h^0 + \gamma_1 h^1 + \gamma_2 h^2 + \dots + \gamma_{k-1} h^{k-1}$ とする。乗算 $r \cdot r'$ は、'の各被加数によって行われる。第1のものは $r \gamma_0 h^0 = X(\alpha \gamma_0)$ であり、この正規化元は第1の乗算入力145である。後のものは、 $i > 0$ での $X \alpha \gamma_i h^i$ である。分配性と $h^k = 1$ であることとを使用した簡単な計算を使用して、 $X \alpha \gamma_i h^i$ の一般表現を得る。この処理は一般表現の $k-1$ 個の加算入力146を生成し、これらは、正規化元である第1の加算入力145のために加算式によって加算される。加算の回数は k と共に増加する。 $k=2$ を使用することは、乗算及び加算が同一の複雑性を有することを意味し、攻撃者がコード内の加算演算と乗算演算とを区別することをより困難にする。

【0107】

一実施形態では、第1の作用群N及び第2の作用群Hは環U(R)の単元群の部分群であり、乗算によって主群に作用し、第2の部分集合 M_0 は主群の単位元のみを含む。

【0108】

図2は計算デバイス101の一実施形態の一例を概略的に示す。計算デバイス101は計算デバイス100'の改良である。一実施形態では、計算デバイス101は、複数の加算ユニットと、複数の乗算ユニットとを備える。たとえば、図2は、3つの乗算ユニット140.1、140.2及び140.3と、2つの加算ユニット130.1及び130.2とを示す。これらのユニットは、それぞれユニット140及び130と同一の設計である。乗算及び加算ユニットは比較的小さいスペースしか取らず、たとえば、ソフトウェアで実装される場合、これらのユニットは数百の低レベルのコンピュータ命令より多い必要はない。具体的には、コンピュータプログラムにおいて必要とされる各乗算又は加算のために、加算及び／又は乗算ユニットのコピーが使用される。これは、従来の難読化手法がこれらのコピーを異ならせて、同一の演算子が使用されていることを攻撃者が知ることができないようにすることを可能にする。たとえば、使用される難読化に応じて、乗算及び／又は加算ユニットが複数の計算に再利用される。一例として、図2は、難読化された算術を使用して多項式 $ax^2 + bx + c$ がどのように計算されるかを示す。

【0109】

10

20

30

40

50

加算、乗算などの複数の算術ユニットの演算は、それらのデータの依存関係によって許容される任意の順序のものである。たとえば、演算 1 4 0 . 3 は、順序 1 4 0 . 1、1 4 0 . 2、1 3 0 . 1、及び 1 3 0 . 2 に、1 3 0 . 1 より前の任意の時点で挿入される。また、その後の乗算又は加算の順序は逆にされてもよい。したがって、図 2 のような図は、多数の方式でソフトウェアプログラムのために線形順序に変換される。ユニットが厳密に分離される必要はなく、第 1 のユニットのための命令には、他のユニットのための命令が散在してもよい。

【0 1 1 0】

図 3 は、計算デバイスで使用される加算テーブルを計算するためのテーブル計算デバイス 2 0 0 の一実施形態の一例を概略的に示す。加算テーブルは、計算デバイス 1 0 0 などのようなデバイスで使用される。加算テーブルは、たとえば、ハードディスク、不揮発性メモリチップなどの非一時的記憶デバイスに記憶される。

10

【0 1 1 1】

テーブル計算デバイス 2 0 0 は、主群 $(M, +)$ の 2 つの元を加算するように構成され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ように構成され、主群は有限アーベル群

【数 5 4】

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

20

である。

【0 1 1 2】

テーブル計算デバイスは、第 2 の部分集合 M_0 の元 m_i についてのルックアップテーブルを構築するように構成されるテーブル作成ユニット 2 1 0 を備える。テーブル作成ユニットは、以下を行うように構成される。

ー 主群 M の入力された正規化元 (γ, X) を繰り返し選択する。たとえば、デバイス 2 0 0 は、正規化元を選択するために、第 1 の作用群及び第 1 の部分集合の元を選択する。

ー 入力された正規化元 γX と第 2 の部分集合の前記元 m_i との和 $s = \gamma X + m_i$ を決定する。この加算は主群 M において行われる。たとえば、入力された正規化元及び m_i の両方が、 M の正準表現に変換される。デバイス 2 0 0 が難読化なしで主群 M において計算することには反対ではなく、その理由は、デバイス 2 0 0 が典型的には計算デバイス 1 0 0 自体の一部ではないためである。

30

ー 第 1 の作用群 N の元 λ と、第 1 の部分集合 Δ の元 Y とを、第 1 の作用群 N の元 λ と、第 1 の部分集合 Δ の元 Y との積が前記和となるように決定する： $\lambda Y h = s = \gamma X + m_i$ 。たとえば、 $s h^{-1}$ を計算し、変換テーブルを使用するなどしてこれを正規化形式に変換する。代替的には、全ての正規化元についての和を計算して、和のテーブルを作成し、次に全ての正規化元 λY にわたってループし、どの和が $\lambda Y h$ と等しいかを決定する。

ー 入力された環の元を第 1 の作用群 N の元 λ と、第 1 の部分集合 Δ の元 Y とに写像するルックアップテーブルにエントリを追加する。

【0 1 1 3】

その結果は、第 2 の部分集合 M_0 の元 m_i についてのテーブルである。テーブル作成は、第 2 の部分集合の他の全ての元について繰り返される。

40

【0 1 1 4】

オペランド記憶装置 1 5 0、加算テーブル記憶装置 1 1 0 などは、電子メモリとして実装される。メモリの一部は揮発性又は不揮発性である。たとえば、それらは S R A M、F L A S H 又は R O M メモリを備える。他の記憶技術、たとえば、磁気記憶装置、クラウド記憶装置なども使用される。好都合なことに、使用される記憶装置は、高速ランダムアクセス、たとえば、緊密に／密接に結合されたメモリを可能にする。

【0 1 1 5】

典型的には、デバイス 1 0 0、1 0 0' 及び 2 0 0 はそれぞれ、デバイスに記憶された

50

適切なソフトウェアを実行するマイクロプロセッサ（別途図示せず）を備え、たとえば、そのソフトウェアは対応するメモリ、たとえばRAMなどの揮発性メモリ、又はフラッシュなどの不揮発性メモリ（別途図示せず）にダウンロード及び／又は記憶される。デバイス100、100'及び200は、マイクロプロセッサ及びメモリ（別途図示せず）が設けられる。代替的には、デバイスは、たとえばフィールドプログラマブルゲートアレイ（FPGA）として、プログラマブルロジックに全体的又は部分的に実装される。デバイス100、100'及び200は、いわゆる特定用途向け集積回路（ASIC）、すなわち、それらの特定の用途向けにカスタマイズされた集積回路（IC）として、全体的又は部分的に実装される。たとえば、回路は、たとえば、Verilog、VHDLなどのハードウェア記述言語を使用して、CMOSに実装される。

10

【0116】

計算の一実施形態は、加算回路、変換回路、関数回路、及び／又は乗算回路などを備える。回路は本明細書に記載された対応するユニットを実装する。回路はプロセッサ回路及び記憶回路であり、プロセッサ回路は記憶回路内で電子的に表される命令を実行する。回路もFPGA、ASICなどである。

【0117】

図3は、主群 $(M, +)$ の2つの元を加算するための電子計算方法300を概略的な形態で示すフローチャートであり、主群は有限アーベル群

【数55】

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

20

である。

【0118】

方法300は以下を有する。

— 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310であって、前記ルックアップテーブルが、主群 (M) の正規化元 (γ, X) を入力として取り、入力を第1の作用群 (N) の元 (λ) と第1の部分集合 (Δ) の元 (Y) とに写像し、第1の作用群 (N) の元 (λ) と第1の部分集合 (Δ) の元 (Y) との積が、正規化元 (γX) と第2の部分集合 (M_0) の前記元 (m_i) との和 $(\lambda Y h = \gamma X + m_i)$ である、記憶するステップ310。たとえば、記憶するステップは、加算テーブルが記憶されるメモリを有することによって実行される。

30

— 第1の加算入力 $(\alpha_0 X_0)$ 及び第2の加算入力

【数56】

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

を受信し、第1及び第2の加算入力の主群 (M) の元であり、第1の加算入力に正規化表現で受信され、第2の加算入力に一般化表現で受信され、第1の加算入力及び第2の加算入力的主群 (M) における和を計算するステップ320であって、

40

— 第2の加算入力の被加数を第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330

を有し、

— 第2の加算入力の被加数

【数57】

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

を部分和に加算するステップ340が、前記被加数における第2の部分集合 (M_0) の元

【数 5 8】

$$m_{i_t}$$

についてのルックアップテーブル

【数 5 9】

$$P_{i_t}$$

を適用するステップを有する、
計算するステップ 3 2 0。

10

【0 1 1 9】

図 5 は、主群 $(M, +)$ の 2 つの元を加算するように構成され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方法 4 0 0 を概略的な形で示すフローチャートを示し、主群は有限アーベル群

【数 6 0】

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

であり、テーブル計算方法は、

20

- 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 (4 1 0) と、
 - 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、第 1 の作用群 (N) の元 (λ) と、第 1 の部分集合 (Δ) の元 (Y) との積が前記和となるように決定するステップ (4 2 0) と、
 - 入力された環の元を第 1 の作用群 (N) の元 (λ) と、第 1 の部分集合 (Δ) の元 (Y) とに写像するルックアップテーブルにエントリを追加するステップ (4 3 0) と
- を有する。

30

【0 1 2 0】

当業者には明らかであるように、本方法を実行する多数の異なる手法が可能である。たとえば、ステップの順序は変更され得、又はいくつかのステップは並行して実行され得る。さらに、ステップの間に、他の方法のステップが挿入され得る。挿入されたステップは、本明細書に記載されるような本方法の改良を表現し、又は本方法と無関係である。また、所与のステップは、次のステップが開始される前に完全に終了していない場合がある。

【0 1 2 1】

本発明による方法は、プロセッサシステムに方法 3 0 0 又は 4 0 0 を実施させるための命令を含むソフトウェアを使用して実行される。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取られるステップのみを含む。ソフトウェアは、ハードディスク、フロッピー、メモリ、光ディスクなどの適切な記憶媒体に記憶される。ソフトウェアは信号としてワイヤに沿って、若しくは無線で、又はインターネットなどのデータネットワークを使用して送信される。ソフトウェアは、ダウンロード及び／又はサーバ上でのリモート使用が可能にされる。本発明による方法は、方法を実施するようにフィールドプログラマブルゲートアレイ (FPGA) などのプログラマブルロジックを構成するようになされるビットストリームを使用して実行される。

40

【0 1 2 2】

本発明が、本発明を実施するようになされたコンピュータプログラム、特に、キャリア上又は内のコンピュータプログラムにも拡張されることは理解されよう。プログラムは、ソースコード、オブジェクトコード、コード中間ソース、及びオブジェクトコード、たと

50

えば部分的にコンパイルされた形式、又は本発明による方法の実装での使用に適した任意の他の形式のものである。コンピュータプログラム製品に関する一実施形態は、記載された方法のうちの少なくとも1つ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命令を含む。これらの命令はサブルーチンに細分され、及び／又は静的若しくは動的にリンクされる1つ又は複数のファイルに記憶される。コンピュータプログラム製品に関する他の実施形態は、記載されたシステム及び／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命令を含む。

【0123】

図6aはコンピュータプログラム1020を含む書き込み可能部分1010を有するコンピュータ可読媒体1000を示し、コンピュータプログラム1020は、プロセッサシステムに一実施形態による主群の2つの元を加算するための計算方法、又は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方法を実施させるための命令を含む。コンピュータプログラム1020は、コンピュータ可読媒体1000上に物理的なマークとして、又はコンピュータ可読媒体1000の磁化によって具現化される。しかしながら、任意の他の適切な実施形態も考えられる。さらに、コンピュータ可読媒体1000はここでは光ディスクとして示されているが、コンピュータ可読媒体1000は、ハードディスク、固体メモリ、フラッシュメモリなどの任意の適切なコンピュータ可読媒体であり、記録不可能又は記録可能であることは理解されよう。コンピュータプログラム1020は、プロセッサシステムに、主群の2つの元を加算するための計算方法、又は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方法である前記方法を実施させるための命令を含む。

【0124】

図6bは一実施形態によるプロセッサシステム1140の概略図を示す。プロセッサシステムは1つ又は複数の集積回路1110を備える。1つ又は複数の集積回路1110のアーキテクチャは図6bに概略的に示されている。回路1110は、一実施形態による方法を実行し、及び／又はそのモジュール若しくはユニットを実装するためにコンピュータプログラムコンポーネントを動作させるための、CPUなどの処理ユニット1120を備える。回路1110は、プログラミングコード、データなどを記憶するためのメモリ1122を備える。メモリ1122の一部は読み出し専用である。回路1110は通信素子1126、たとえば、アンテナ、コネクタ又はその両方などを備える。回路1110は、本方法で定義された処理の一部又は全部を実施するための専用集積回路1124を備える。プロセッサ1120、メモリ1122、専用IC1124及び通信素子1126は相互接続1130、たとえばバスを介して互いに接続される。プロセッサシステム1110は、アンテナ及び／又はコネクタを使用して、それぞれ接触及び／又は非接触通信用に構成される。

【0125】

上記の実施形態は本発明を限定するものではなく例示するものであり、当業者は多くの代替的实施形態を設計できることに留意されたい。

【0126】

特許請求の範囲において、括弧内に置かれた任意の参照符号は、請求項を限定するものとして解釈されるべきではない。「備える」という動詞及びその活用形の使用は、請求項に記述された以外の要素又はステップの存在を排除するものではない。要素に先行する冠詞「a」又は「an」は、複数のそのような要素の存在を排除するものではない。本発明は、いくつかの個別の素子を含むハードウェアによって、及び適切にプログラムされたコンピュータによって実装される。いくつかの手段を列挙したデバイスの請求項において、これらの手段のいくつかは、同一のハードウェア項目によって具現化される。特定の対策が相異なる従属請求項に列挙されているという単なる事実は、これらの対策の組み合わせが有利に使用できないことを示すものではない。

【0127】

特許請求の範囲において、括弧内の参照は、実施形態の図面における参照符号又は実施

10

20

30

40

50

形態の式を参照して、請求項の明瞭性を高めている。これらの参照は請求項を限定するものとして解釈されるべきではない。

【符号の説明】

【0128】

図1a～図1dの参照番号のリスト：

100	計算デバイス	
110	加算テーブル記憶装置	
122	変換ユニット	
124	関数ユニット	
130	加算ユニット	10
131	第1の加算入力	
132	第2の加算入力	
133	部分和	
134	部分加算ユニット	
140	乗算ユニット	
141	第1の乗算入力	
142	第2の乗算入力	
144	中間乗算ユニット	
145	第1の加算入力	
146	1つ又は複数の第2の加算入力	20
150	オペランド記憶装置	
152	定数記憶装置	
160	復号ユニット	
170	符号化ユニット	
171	直接入力	
172	符号化テーブルを記憶するように構成される記憶装置	

【図 1 a】

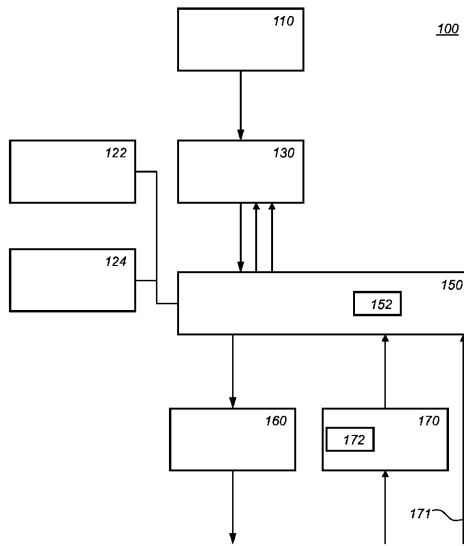


Fig. 1a

【図 1 b】

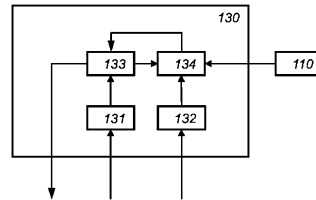


Fig. 1b

【図 1 c】

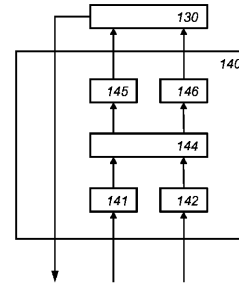


Fig. 1c

【図 1 d】

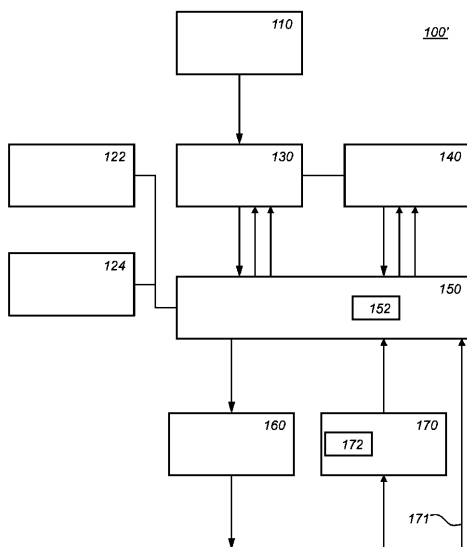


Fig. 1d

【図 2】

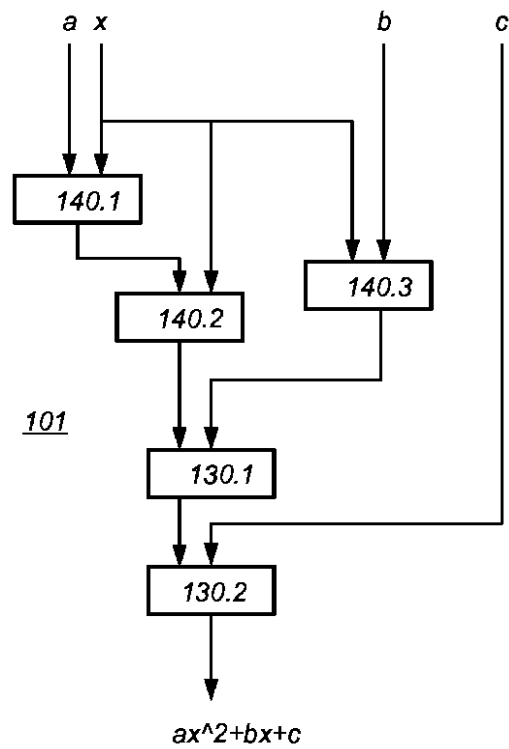
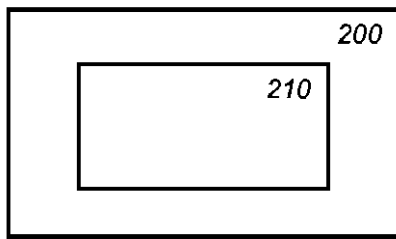
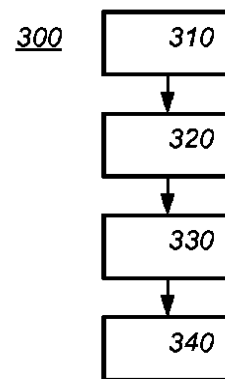


Fig. 2

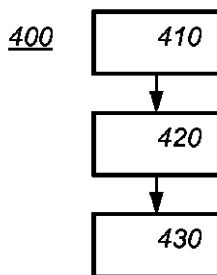
【図 3】

*Fig. 3*

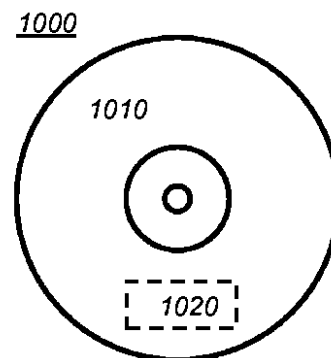
【図 4】

*Fig. 4*

【図 5】

*Fig. 5*

【図 6 a】

*Fig. 6a*

【図 6 b】

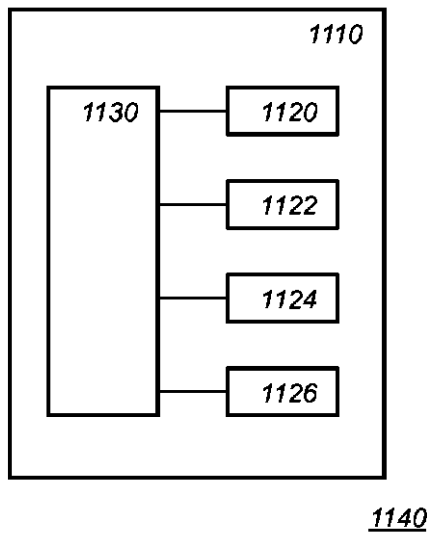


Fig. 6b

【手続補正書】

【提出日】平成30年1月31日(2018.1.31)

【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 $\underline{\text{の難読化された加算のための電子計算デバイスであって}}$ 、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 = 〈h〉）、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 = n X）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 3】

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

）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 2】

$$m_{i_t}$$

）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 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 乃至 3 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 乃至 4 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 乃至 5 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 乃至 6 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 乃至 7 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 1 0】

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 乃至 9 のいずれか一項に記載の電子計算デバイス。

【請求項 1 1】

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 の加算入力の前記主群の元

【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 ($\alpha_t X_t$) から次の部分 ($\alpha_{t+1} X_{t+1}$) を取得し、 γ^{-1} が前記主群 (M) の単位元であり、 $\alpha_t X_t$ が前記現在の部分であり、

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

請求項 10 に記載の電子計算デバイス。

【請求項 1 2】

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 乃至 11 のいずれか一項に記載の電子計算デバイス。

【請求項 1 3】

前記主群 ($(M, +)$) が、前記主群を環 ($(R, +, \cdot)$) にするさらなる演算 ($\cdot$) 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 の乗算入力の前記主環 (R) の元であり、前記第 1 の乗算入力正規化表現 ($(\beta_0 h^0 + \cdots \beta_{k-2} h^{k-2} + h^{k-1}) \alpha = X \alpha$) 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 の加算入力一般化形式 $(X(\alpha \gamma_i)h^i = (Xh^i)n')$ 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 1 2 に記載の電子計算デバイス。

【請求項 1 4】

$(\#N \cdot \#M_0) \#H \geq 3/2 (\#N \cdot \#\Delta)$ 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 乃至 1 3 のいずれか一項に記載の電子計算デバイス。

【請求項 1 5】

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 7 7】

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

であり、

前記第 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 $((\gamma, X))$ 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、

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 1 6】

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 7 8】

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

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 ($H = (h)$)、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 (

【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 の加算入力の前記主群 (M) の元であり、前記第 1 の加算入力前記正規化表現で受信され、前記第 2 の加算入力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方法であって、前記主群が有限アーベル群（

【数 8 5】

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

）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（ $\lambda Y h = \gamma X + m_i$ ）を決定するステップと、

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 又は 17 に記載の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。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/079971

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F17/10 G06F21/14 H04L9/06
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)

G06F 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	WO 2010/102960 A1 (IRDETO BV [NL]; MICHIELS WILHELMUS PETRUS ADRIANUS JOHANNUS [NL]; GORI) 16 September 2010 (2010-09-16) page 6 - page 7 -----	1-19
X	US 2015/312039 A1 (MICHIELS WIL [NL] ET AL) 29 October 2015 (2015-10-29) page 4 - page 7 -----	1-19
X	WO 2010/146140 A1 (IRDETO BV [NL]; MICHIELS WILHELMUS PETRUS ADRIANUS JOHANNUS [NL]) 23 December 2010 (2010-12-23) page 13 - page 21 ----- -/-	1-19

☒ 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

17 February 2017

Date of mailing of the international search report

27/02/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel: (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Huguet Serra, G

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2016/079971

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105 099 666 A (INST INF ENG CAS) 25 November 2015 (2015-11-25) pages 4, 6, 8 and 9 -----	1-19
X	Alan C Lin: "SOFTWARE OBFUSCATION WITH SYMMETRIC CRYPTOGRAPHY", March 2008 (2008-03), XP055080966, Retrieved from the Internet: URL:http://www.dtic.mil/dtic/tr/fulltext/u 2/a486850.pdf [retrieved on 2013-09-25] page 37 - page 48 -----	1-19
X	Martin Tehan: "White-Box Cryptography", 24 June 2013 (2013-06-24), XP055080911, Retrieved from the Internet: URL:http://is.muni.cz/th/207885/fi_m/thesi s_tehan.pdf [retrieved on 2013-09-25] Chapter 3 -----	1-19
A	Lee Badger ET AL: "Self-Protecting Mobile Agents Obfuscation Techniques Evaluation Report", Report #01-036, 30 November 2001 (2001-11-30), XP055314284, Retrieved from the Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/d ownload?doi=10.1.1.127.3668&rep=rep1&type= pdf [retrieved on 2016-10-26] the whole document -----	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/079971

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010102960 A1	16-09-2010	CA 2754094 A1	16-09-2010
		CN 102461058 A	16-05-2012
		EP 2406916 A1	18-01-2012
		JP 5688528 B2	25-03-2015
		JP 2012520589 A	06-09-2012
		KR 20120030335 A	28-03-2012
		US 2012002807 A1	05-01-2012
		WO 2010102960 A1	16-09-2010

US 2015312039 A1	29-10-2015	CN 105024803 A	04-11-2015
		US 2015312039 A1	29-10-2015

WO 2010146140 A1	23-12-2010	NONE	

CN 105099666 A	25-11-2015	NONE	

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, ST, 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, KM, 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA

(72)発明者 マリン レアンドロ

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

Fターム(参考) 5B056 BB72