

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7173328号

(P7173328)

(45)発行日 令和4年11月16日(2022.11.16)

(24)登録日 令和4年11月8日(2022.11.8)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62 3 1 8

G 0 6 F 21/71 (2013.01)

G 0 6 F 21/71

G 0 6 F 7/535(2006.01)

G 0 6 F 7/535

請求項の数 6 (全9頁)

(21)出願番号 特願2021-525410(P2021-525410)

(86)(22)出願日 令和1年6月10日(2019.6.10)

(86)国際出願番号 PCT/JP2019/022895

(87)国際公開番号 WO2020/250269

(87)国際公開日 令和2年12月17日(2020.12.17)

審査請求日 令和3年11月19日(2021.11.19)

(73)特許権者 000004226

日本電信電話株式会社

東京都千代田区大手町一丁目5番1号

(74)代理人 100121706

弁理士 中尾 直樹

(74)代理人 100128705

弁理士 中村 幸雄

(74)代理人 100147773

弁理士 義村 宗洋

(72)発明者 濱田 浩気

東京都千代田区大手町一丁目5番1号

日本電信電話株式会社内

審査官 中里 裕正

最終頁に続く

(54)【発明の名称】 秘密除算システム、秘密計算装置、秘密除算方法、およびプログラム

(57)【特許請求の範囲】

【請求項1】

Rを3以上の整数とし、 L_0 、 L_1 を非負の整数とし、Nを0以上 R^{L_1} 未満の実数とし、Dを自然数とし、 $N \cdot L_0$ 、 $\dots$ 、 $N \cdot L_{L_1-1}$ をNのR進法での小数点以下 L_0 桁目から整数部 L_1 桁目までの各桁の値とし、jを L_1-1 から L_0 までの各整数とし、

複数の秘密計算装置を含み、Nの秘匿値[N]とDの秘匿値[D]を用いてNをDで除算した結果を表す秘匿値を得る秘密除算システムであって、

上記秘密計算装置は、

部分剰余 P_{L_1} の秘匿値 $[P_{L_1}]$ を0に設定する初期化部と、

部分除数 $n = P_{j+1}R + N_j$ の秘匿値[n]と1以上R未満の各整数gについての $[D] \times g$ とを並列に比較した比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を計算する並列比較部と、

上記比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を用いて $n = DQ_j + P_j$ を満たす商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを計算する更新部と、

を含む秘密除算システム。

【請求項2】

請求項1に記載の秘密除算システムであって、

上記並列比較部は、次式によりgについての比較結果 E_g の秘匿値 $[E_g]$ を計算する、

【数7】

10

$$[E_g] = ([D] \times g \leq [n])$$

秘密除算システム。

【請求項 3】

請求項 1 または 2 に記載の秘密除算システムであって、
上記更新部は、次式により商 Q_j の秘匿値 $[Q_j]$ を計算し、

【数 8】

$$[Q_j] := [E_1] + \dots + [E_{R-1}]$$

10

次式により部分剰余 P_j の秘匿値 $[P_j]$ を計算する、

【数 9】

$$[P_j] := [n] - [D] \times [Q_j]$$

秘密除算システム。

【請求項 4】

R を 3 以上の整数とし、 L_0, L_1 を非負の整数とし、 N を 0 以上 R^{L_1} 未満の実数とし、 D を自然数とし、 $N_{-L_0}, \dots, N_{L_1-1}$ を N の R 進法での小数点以下 L_0 桁目から整数部 L_1 桁目までの各桁の値とし、 j を L_1-1 から $-L_0$ までの各整数とし、

N の秘匿値 $[N]$ と D の秘匿値 $[D]$ を用いて N を D で除算した結果を表す秘匿値を得る秘密除算システムで用いられる秘密計算装置であって、

20

部分剰余 P_{L_1} の秘匿値 $[P_{L_1}]$ を 0 に設定する初期化部と、

部分除数 $n = P_{j+1}R + N_j$ の秘匿値 $[n]$ と 1 以上 R 未満の各整数 g についての $[D] \times g$ とを並列に比較した比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を計算する並列比較部と、

上記比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を用いて $n = DQ_j + P_j$ を満たす商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを計算する更新部と、

を含む秘密計算装置。

【請求項 5】

R を 3 以上の整数とし、 L_0, L_1 を非負の整数とし、 N を 0 以上 R^{L_1} 未満の実数とし、 D を自然数とし、 $N_{-L_0}, \dots, N_{L_1-1}$ を N の R 進法での小数点以下 L_0 桁目から整数部 L_1 桁目までの各桁の値とし、 j を L_1-1 から $-L_0$ までの各整数とし、

30

複数の秘密計算装置を含み、 N の秘匿値 $[N]$ と D の秘匿値 $[D]$ を用いて N を D で除算した結果を表す秘匿値を得る秘密除算システムが実行する秘密除算方法であって、

各秘密計算装置の初期化部が、部分剰余 P_{L_1} の秘匿値 $[P_{L_1}]$ を 0 に設定し、

各秘密計算装置の並列比較部が、部分除数 $n = P_{j+1}R + N_j$ の秘匿値 $[n]$ と 1 以上 R 未満の各整数 g についての $[D] \times g$ とを並列に比較した比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を計算し、

各秘密計算装置の更新部が、上記比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を用いて $n = DQ_j + P_j$ を満たす商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを計算する、

秘密除算方法。

40

【請求項 6】

請求項 4 に記載の秘密計算装置としてコンピュータを機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、暗号応用技術に関し、特に入力や出力の値を明かすことなく除算を効率よく行う技術に関する。

【背景技術】

【0002】

暗号化された数値を復元することなく特定の演算結果を得る方法として、秘密計算と呼

50

ばれる方法がある（例えば、非特許文献 1 参照）。非特許文献 1 に記載された方法では、3つの秘密計算装置に数値の断片を分散させるという暗号化を行い、3つの秘密計算装置が協調計算を行うことにより、数値を復元することなく、加減算、定数加算、乗算、定数倍、論理演算（否定、論理積、論理和、排他的論理和）、データ形式変換（整数、二進数）の結果を3つの秘密計算装置に分散された状態、すなわち暗号化されたまま保持させることができる。

【0003】

入力や出力の値を明かすことなく除算を行う場合、ゴールドシュミット除算を秘密計算で実現する方法がある（例えば、非特許文献 2 参照）。

【先行技術文献】

【非特許文献】

【0004】

【文献】千田浩司、濱田浩気、五十嵐大、高橋克巳、“軽量検証可能3パーティ秘匿関数計算の再考”、CSS、2010年

Dan Bogdanov, Margus Niitsoo, Tomas Toft, and Jan Willemson, "High-performance secure multi-party computation for data mining applications," International Journal of Information Security, Vol. 11, No. 6, pp. 403-418, 2012.

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、ゴールドシュミット除算を秘密計算で実現する場合、固定小数点数の乗算を使う必要がある。秘密計算では固定小数点数の乗算は処理段数すなわち通信回数が多いという問題がある。

【0006】

この発明の目的は、上記のような技術的課題に鑑みて、固定小数点数の乗算を使わず、少ない処理段数で除算を実現することである。

【課題を解決するための手段】

【0007】

上記の課題を解決するために、この発明の一態様の秘密除算システムは、 R を3以上の整数とし、 L_0, L_1 を非負の整数とし、 N を0以上 R^{L_1} 未満の実数とし、 D を自然数とし、 $N_{-L_0}, \dots, N_{L_1-1}$ を N の R 進法での小数点以下 L_0 桁目から整数部 L_1 桁目までの各桁の値とし、 j を L_1-1 から $-L_0$ までの各整数とし、複数の秘密計算装置を含み、 N の秘匿値 $[N]$ と D の秘匿値 $[D]$ を用いて N を D で除算した結果を表す秘匿値を得る秘密除算システムであって、秘密計算装置は、部分剰余 P_{L_1} の秘匿値 $[P_{L_1}]$ を0に設定する初期化部と、部分除数 $n=P_{j+1}R+N_j$ の秘匿値 $[n]$ と1以上 R 未満の各整数 g についての $[D] \times g$ とを並列に比較した比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を計算する並列比較部と、比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を用いて $n=DQ_j+P_j$ を満たす商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを計算する更新部と、を含む。

【発明の効果】

【0008】

この発明によれば、固定小数点数の乗算を使わず除算を実現するため、少ない処理段数で除算を実現できる。

【図面の簡単な説明】

【0009】

【図1】図1は、秘密除算システムの機能構成を例示する図である。

【図2】図2は、秘密計算装置の機能構成を例示する図である。

【図3】図3は、秘密除算方法の処理手続きを例示する図である。

【図4】図4は、コンピュータの機能構成を例示する図である。

【発明を実施するための形態】

【0010】

10

20

30

40

50

はじめに、この明細書における表記方法および用語の定義について説明する。

【0011】

<表記方法>

ある値 a を暗号化や秘密分散などにより秘匿化した値を a の秘匿値と呼び、 $[a]$ と表記する。秘匿化が秘密分散である場合は、 $[a]$ により各秘密計算装置が持つ秘密分散の断片の集合を参照する。

【0012】

変数の定義域における $[a, b]$ （角括弧）は閉区間を表し、 (a, b) （丸括弧）は开区間を表す。例えば、 $i \in [a, b]$ は i が a 以上 b 以下の値を取ることを表す。また、 $i \in (a, b)$ は i が a 以上 b 未満の値を取ることを表す。

10

【0013】

<加算、減算、乗算>

秘匿文に対する加算、減算、乗算の各演算は、2つの値 a, b の秘匿値 $[a], [b]$ を入力とし、それぞれ $a+b, a-b, ab$ の計算結果 c_1, c_2, c_3 の秘匿値 $[c_1], [c_2], [c_3]$ を計算する。これらの演算の実行をそれぞれ次式のように記述する。

【0014】

【数1】

$$[c_1] \leftarrow \text{Add}([a], [b]),$$

$$[c_2] \leftarrow \text{Sub}([a], [b]),$$

$$[c_3] \leftarrow \text{Mul}([a], [b])$$

20

【0015】

誤解を招く恐れのない場合は、 $\text{Add}([a], [b]), \text{Sub}([a], [b]), \text{Mul}([a], [b])$ をそれぞれ $[a]+[b], [a]-[b], [a] \times [b]$ と略記する。

【0016】

<比較>

比較の演算は、2つの値 a, b の秘匿値 $[a], [b]$ を入力とし、 $a \leq b$ の真偽値 $c \in \{0, 1\}$ の秘匿値 $[c]$ を計算する。真偽値は真のとき1、偽のとき0とする。この演算の実行を次式のように記述する。

30

【0017】

【数2】

$$[c] \leftarrow ([a] \overset{?}{\leq} [b])$$

【0018】

以下、この発明の実施の形態について詳細に説明する。なお、図面中において同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

【0019】

〔実施形態〕

40

実施形態の秘密除算システムは、被除数 N の秘匿値 $[N]$ と除数 D の秘匿値 $[D]$ とを入力とし、 N/D の R 進法での小数点以下の L_0 桁目から整数部 L_1 桁目までの各桁の値 $Q_{-L_0}, \dots, Q_{L_1-1}$ の秘匿値 $[Q_{-L_0}], \dots, [Q_{L_1-1}]$ を計算して出力する。ここで、 R は3以上の整数、 L_0, L_1 は非負の整数、 N は0以上 R^{L_1} 未満の実数、 D は自然数とする。なお、実施形態中で用いる $[N_{-L_0}], [N_{-L_0+1}], \dots, [N_{L_1-2}], [N_{L_1-1}]$ は、次式のように N の R 進分解を表す $N_{-L_0}, N_{-L_0+1}, \dots, N_{L_1-2}, N_{L_1-1}$ の秘匿値である。

【0020】

【数3】

50

$$N_{-L_0}, N_{-L_0+1}, \dots, N_{L_1-2}, N_{L_1-1}$$

$$\text{s.t. } N = \sum_{j \in [-L_0, L_1)} N_j R^j + r, 0 \leq r < R^{-L_0}, N_j \in [0, R)$$

【0021】

図1を参照して、実施形態の秘密除算システムの構成例を説明する。秘密除算システム100は、例えば、図1に示すように、 K (≥ 2) 台の秘密計算装置11, ..., 1 $_K$ を含む。本実施形態では、秘密計算装置11, ..., 1 $_K$ はそれぞれ通信網9へ接続される。通信網9は、接続される各装置が相互に通信可能なように構成された回線交換方式もしくはパケット交換方式の通信網であり、例えばインターネットやLAN (Local Area Network)、WAN (Wide Area Network) などを用いることができる。なお、各装置は必ずしも通信網9を介してオンラインで通信可能である必要はない。例えば、秘密計算装置11, ..., 1 $_K$ へ入力する情報を磁気テープやUSBメモリなどの可搬型記録媒体に記憶し、その可搬型記録媒体から秘密計算装置11, ..., 1 $_K$ へオフラインで入力するように構成してもよい。

【0022】

図2を参照して、実施形態の秘密除算システム100に含まれる秘密計算装置1 $_k$ ($k=1, \dots, K$) の構成例を説明する。秘密計算装置1 $_k$ は、例えば、図2に示すように、入力部11、初期化部12、並列比較部13、更新部14、反復制御部15、および出力部16を含む。この秘密計算装置1 $_k$ ($k=1, \dots, K$) が他の秘密計算装置1 $_{k'}$ ($k'=1, \dots, K$ 、ただし $k \neq k'$) と協調しながら後述する各ステップの処理を行うことにより本形態の秘密除算方法が実現される。

【0023】

秘密計算装置1 $_k$ は、例えば、中央演算処理装置 (CPU: Central Processing Unit)、主記憶装置 (RAM: Random Access Memory) などを含む公知又は専用のコンピュータに特別なプログラムが読み込まれて構成された特別な装置である。秘密計算装置1 $_k$ は、例えば、中央演算処理装置の制御のもとで各処理を実行する。秘密計算装置1 $_k$ に入力されたデータや各処理で得られたデータは、例えば、主記憶装置に格納され、主記憶装置に格納されたデータは必要に応じて中央演算処理装置へ読み出されて他の処理に利用される。秘密計算装置1 $_k$ の各処理部は、少なくとも一部が集積回路等のハードウェアによって構成されていてもよい。

【0024】

図3を参照して、実施形態の秘密除算システム100が実行する秘密除算方法の処理手続きを説明する。

【0025】

ステップS11において、各秘密計算装置1 $_k$ の入力部11へ被除数 N の秘匿値 $[N]$ と除数 D の秘匿値 $[D]$ とが入力される。被除数 N の秘匿値 $[N]$ の代わりに、被除数 N の R 進分解を表す $N_{-L_0}, N_{-L_0+1}, \dots, N_{L_1-2}, N_{L_1-1}$ の秘匿値 $[N_{-L_0}], \dots, [N_{L_1-1}]$ が入力部11へ入力されてもよい。入力部11へ被除数 N の秘匿値 $[N]$ が入力された場合、入力部11は、被除数 N の秘匿値 $[N]$ から被除数 N の R 進分解を表す $N_{-L_0}, N_{-L_0+1}, \dots, N_{L_1-2}, N_{L_1-1}$ の秘匿値 $[N_{-L_0}], \dots, [N_{L_1-1}]$ を生成する。入力部11は、被除数 N の R 進分解を表す $N_{-L_0}, N_{-L_0+1}, \dots, N_{L_1-2}, N_{L_1-1}$ の秘匿値 $[N_{-L_0}], \dots, [N_{L_1-1}]$ と除数 D の秘匿値 $[D]$ とを並列比較部13へ出力する。

【0026】

ステップS12において、各秘密計算装置1 $_k$ の初期化部12は、部分剰余 P_{L_1} の秘匿値 $[P_{L_1}]$ を $[P_{L_1}]=0$ に初期化する。また、反復処理のインデックス j を $j=L_1-1$ に初期化する。初期化部12は、部分剰余 P_{L_1} の秘匿値 $[P_{L_1}]$ を並列比較部13へ出力する。また、インデックス j を反復制御部15へ出力する。

【0027】

ステップS13において、各秘密計算装置1 $_k$ の並列比較部13は、 $n=P_{j+1}R+N_j$ である部分除数 n の秘匿値 $[n]$ と、 $g \in [1, R)$ である各 $[D] \times g$ とをそれぞれ並列に比較した結果 E_g

の秘匿値 $[E_g]$ ($g \in [1, R]$)を計算する。具体的には、並列比較部 1 3 は、次式により、1以上 R 未満の各整数 g について比較結果 E_g の秘匿値 $[E_g]$ を計算する。並列比較部 1 3 は、比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を更新部 1 4 へ出力する。

【0028】

【数4】

$$[E_g] = ([D] \times g \leq [n]) \text{ for } g \in [1, R]$$

【0029】

ステップS 1 4において、各秘密計算装置 1 k の更新部 1 4 は、比較結果 $E_1, \dots, E_{R-1}$ の秘匿値 $[E_1], \dots, [E_{R-1}]$ を用いて、商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを計算する。なお、 Q_j と P_j は $n = DQ_j + P_j$, $Q_j \in [0, R)$, $P_j \in [0, R)$ を満たす。具体的には、更新部 1 4 は、次式により商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを計算する。更新部 1 4 は、商 Q_j の秘匿値 $[Q_j]$ と部分剰余 P_j の秘匿値 $[P_j]$ とを出力部 1 6 へ出力する。

【0030】

【数5】

$$[Q_j] := [E_1] + \dots + [E_{R-1}],$$

$$[P_j] := [n] - [D] \times [Q_j]$$

【0031】

ステップS 1 5-1において、各秘密計算装置 1 k の反復制御部 1 5 は、 j が $-L_0$ 以下となっているか否か、すなわち $j \leq -L_0$ の真偽を判定する。 $j \leq -L_0$ が偽、すなわち $j > -L_0$ であれば、ステップS 1 5-2へ処理を進める。 $j \leq -L_0$ が真であれば、ステップS 1 6へ処理を進める。ステップS 1 5-2において、各秘密計算装置 1 k の反復制御部 1 5 は、 j をデクリメント、すなわち $j = j - 1$ を計算し、ステップS 1 3へ処理を戻す。言い替えると、反復制御部 1 5 は、 $j = L_1 - 1, \dots, -L_0$ の各 j について並列比較部 1 3 と更新部 1 4 を繰り返し実行する制御を行う。

【0032】

ステップS 1 6において、各秘密計算装置 1 k の出力部 1 6 は、商 $Q_{-L_0}, \dots, Q_{L_1-1}$ の秘匿値 $[Q_{-L_0}], \dots, [Q_{L_1-1}]$ を出力する。

【0033】

上述した実施形態で実行するアルゴリズムを以下に示す。

【0034】

【数6】

$$1. [P_{L_1}] = 0$$

$$2. \text{ for } j = L_1 - 1 \text{ to } -L_0 \text{ do}$$

$$(a) [n] := [P_{j+1}] \times R + [N_j]$$

$$(b) [E_g] = ([D] \times g \leq [n]) \text{ for } g \in [1, R]$$

$$(c) [Q_j] := [E_1] + \dots + [E_{R-1}], [P_j] := [n] - [D] \times [Q_j]$$

【0035】

上記実施形態の構成では、 $L_0 + L_1$ 段の比較で除算を実現できる。1回の除算で要する段数が小さいため、特に、除算を直列に繰り返し実行するとき実行時間が短くなる。

【0036】

上記実施形態で $R=2$ とした場合、ビット単位で除算を計算することに相当する。ビット単位で計算される除算は比較の段数が大きい。上記実施形態では、比較の回数はビット単

10

20

30

40

50

位で計算される除算と比較して約 $(R-1)/(\log_2 R)$ 倍に増えるものの、段数を約 $1/(\log_2 R)$ 倍に小さくすることができる。

【0037】

以上、この発明の実施の形態について説明したが、具体的な構成は、これらの実施の形態に限られるものではなく、この発明の趣旨を逸脱しない範囲で適宜設計の変更等があっても、この発明に含まれることはいうまでもない。実施の形態において説明した各種の処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【0038】

〔プログラム、記録媒体〕

上記実施形態で説明した各装置における各種の処理機能をコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムを図4に示すコンピュータの記憶部1020に読み込ませ、制御部1010、入力部1030、出力部1040などに動作させることにより、上記各装置における各種の処理機能がコンピュータ上で実現される。

【0039】

この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等のようなものでもよい。

【0040】

また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

【0041】

このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記憶装置に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

【0042】

また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、本装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

10

20

30

40

50

【図面】

【図 1】

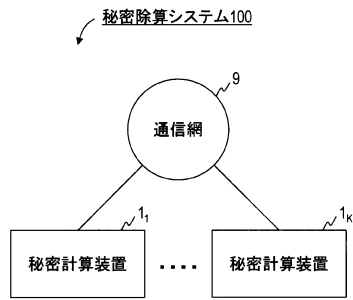


図 1

【図 2】

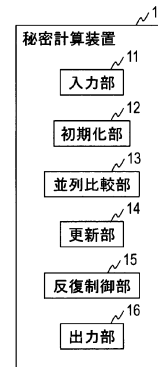


図2

【図 3】

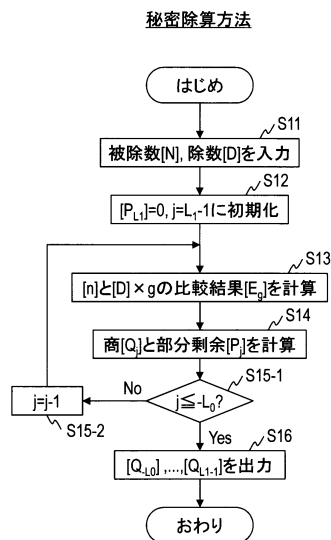


図3

【図 4】

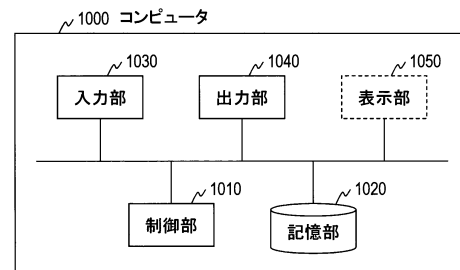


図4

10

20

30

40

50

フロントページの続き

- (56)参考文献 国際公開第2016/129363 (WO, A1)
CATRINA, O. and DRAGULIN, C., Multiparty Computation of Fixed-Point Multiplication and Reciprocal, 20th International Workshop on Database and Expert System Application, 2009年, pp.107-111
ALIASGARI, M. et al., Secure Computation on Floating Point Numbers, Cryptology ePrint Archive, Paper 2012/405 ver.20121210:185402, [online], 2012年12月, pp.1-31, URL:<https://eprint.iacr.org/2012/405/20121210:185402>
- (58)調査した分野 (Int.Cl., DB名)
G06F 21/62
G06F 21/71
G06F 7/535
JSTPlus/JMEDPlus/JST7580 (JDreamII)
IEEE Xplore