

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2018年7月26日(26.07.2018)



(10) 国際公開番号

WO 2018/135566 A1

- (51) 国際特許分類:
G09C 1/00 (2006.01) *G06F 7/552* (2006.01)
- (21) 国際出願番号: PCT/JP2018/001346
- (22) 国際出願日: 2018年1月18日(18.01.2018)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2017-008094 2017年1月20日(20.01.2017) JP
- (71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).
- (72) 発明者: 濱田 浩気(HAMADA, Koki); 〒1808585 東京都武蔵野市緑町三丁目9番11号 N T T 知的財産センタ内 Tokyo (JP).
- (74) 代理人: 中尾 直樹, 外 (NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目1番22号 新宿NSOビル6階 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): 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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) Title: SECURE COMPUTING SYSTEM, SECURE COMPUTING DEVICE, SECURE COMPUTING METHOD, AND PROGRAM

(54) 発明の名称: 秘密計算システム、秘密計算装置、秘密計算方法、プログラム

【図4】

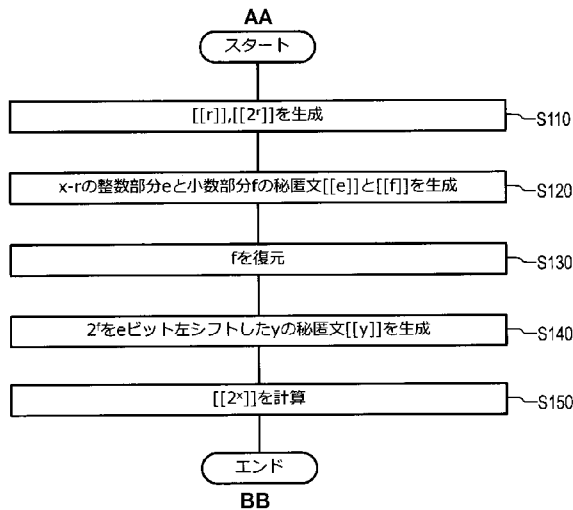


Fig. 4

S110 Generate $[[r]]$, $[[2^r]]$

S120 Generate the concealed texts $[[e]]$ and $[[f]]$ of the integer part e and the decimal part f of $x-r$,

S130 Restore f

S140 Generate the concealed text $[[y]]$ of y obtained by left shifting 2^f by e bits

S150 Calculate $[[2^x]]$

AA Start

BB End

(57) Abstract: A secure computing technique is provided for calculating powers of two in a shorter computation time. This secure computing system includes: a decimal decomposition means 120 which uses a concealed text $[[r]]$ to calculate, from a concealed text $[[x]]$, a concealed text $[[x]]-[[r]]$ of the difference $x-r$ between the value x and a random number r , and generates, from the concealed texts $[[x]]-[[r]]$, a concealed text $[[e]]$, $[[f]]$ of the integer part e and the decimal part f ($0 \leq f < 1$) of the difference $x-r$; a restoring means 130 which restores the decimal part f from the concealed text $[[f]]$; a left shifting means 140 which, from the decimal part f and the concealed text $[[e]]$, generates a concealed text $[[y]]$ of a left-shifted value y , which is the value obtained by left shifting, by e bits, 2^f , i.e., the power of two with the decimal part f as the exponent; and an



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,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告 (条約第21条(3))

exponentiation calculation means 150 which, from the concealed text $[[y]]$, uses the concealed text $[[2^r]]$ to calculate, as the concealed text $[[2^x]]$, a concealed text $[[2^r]] \times [[y]]$ of the value $2^r \times y$, obtained by multiplying the power of two 2^r and the left shifted value y .

(57) 要約: より小さい計算時間で2のべき乗を計算する秘密計算技術を提供する。秘匿文 $[[r]]$ を用いて、秘匿文 $[[x]]$ から値 x と乱数 r の差 $x-r$ の秘匿文 $[[x]]-[[r]]$ を計算し、秘匿文 $[[x]]-[[r]]$ から差 $x-r$ の整数部分 e と小数部分 $f(0 \leq f < 1)$ の秘匿文 $[[e]], [[f]]$ を生成する小数分解手段120と、秘匿文 $[[f]]$ から、小数部分 f を復元する復元手段130と、小数部分 f と秘匿文 $[[e]]$ から、小数部分 f の2のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]]$ を生成する左シフト手段140と、秘匿文 $[[2^r]]$ を用いて、秘匿文 $[[y]]$ から2のべき乗 2^r と左シフト値 y を乗算した値 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を秘匿文 $[[2^x]]$ として計算するべき乗計算手段150とを含む。

明 細 書

発明の名称：

秘密計算システム、秘密計算装置、秘密計算方法、プログラム

技術分野

[0001] 本発明は、秘密計算技術に関するものであり、特に、入力値を秘密にしたまま2のべき乗を計算する秘密計算技術に関する。

背景技術

[0002] 暗号化された数値を復元することなく指定された演算の演算結果を得る方法として、秘密計算と呼ばれる方法がある（例えば非特許文献1参照）。非特許文献1の方法では、数値を復元することのできる複数の情報（数値の断片）を3つの秘密計算装置に分散するという暗号化を行い、数値を復元することなく、加減算、定数和、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。一般に、分散数は3に限らず W （ W は2以上の所定の定数）とすることができ、 W 個の秘密計算装置による協調計算によって秘密計算を実現するプロトコルはマルチパーティプロトコルと呼ばれる。

[0003] なお、分散数が2の場合の秘密計算方法については、例えば、非特許文献2に開示されている。

[0004] 秘密計算によって指数関数の計算を実現した方法として、非特許文献3の方法がある。非特許文献3の方法では、まず2のべき乗を求めたい値を整数部分 e と小数部分 f （ $0 \leq f < 1$ ）に分解、それぞれの2のべき乗 2^e と 2^f を計算し、 2^e と 2^f の積を求めることにより、指数関数の計算を実現している。

先行技術文献

非特許文献

[0005] 非特許文献1：千田浩司，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”，情報処理学会シンポジウム論文集，Vol.201

0, No.9, pp.555-560, 2010.

非特許文献2: Ivan Damgard, Valerio Pastro, Nigel Smart, Sarah Zakarias, "Multiparty Computation from Somewhat Homomorphic Encryption", CRYPTO 2012, LNCS7417, pp.643-662, 2012.

非特許文献3: Liina Kamm, Jan Willemson, "Secure floating point arithmetic and private satellite collision analysis", International Journal of Information Security, Vol.14, No.6, pp.531-548, 2015.

発明の概要

発明が解決しようとする課題

[0006] しかしながら、非特許文献3の方法では、小数部分 f の2のべき乗 2^f を計算する際、 f の4次多項式の計算をする必要があるため、計算時間が大きくなるという問題があった。

[0007] そこで本発明は、より小さい計算時間で2のべき乗を計算する秘密計算技術を提供することを目的とする。

課題を解決するための手段

[0008] 本発明の一態様は、 r を $0 \leq r < 1$ を満たす乱数、 $[[r]]$ を前記乱数 r の秘匿文、 $[[2^r]]$ を前記乱数 r の2のべき乗 2^r の秘匿文とし、2個以上の秘密計算装置で構成され、2のべき乗を計算する値 x の秘匿文 $[[x]]$ から、前記値 x の2のべき乗 2^x の秘匿文 $[[2^x]]$ を計算する秘密計算システムであって、前記秘匿文 $[[r]]$ を用いて、前記秘匿文 $[[x]]$ から前記値 x と前記乱数 r の差 $x-r$ の秘匿文 $[[x]]-[[r]]$ を計算し、前記秘匿文 $[[x]]-[[r]]$ から前記差 $x-r$ の整数部分 e と小数部分 f ($0 \leq f < 1$)の秘匿文 $[[e]]$, $[[f]]$ を生成する小数分解手段と、前記秘匿文 $[[f]]$ から、前記小数部分 f を復元する復元手段と、前記小数部分 f と前記秘匿文 $[[e]]$ から、前記小数部分 f の2のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]]$ を生成する左シフト手段と、前記秘匿文 $[[2^r]]$ を用いて、前記秘匿文 $[[y]]$ から前記2のべき乗 2^r と前記左シフト値 y を乗算した値 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を前記秘匿文 $[[2^x]]$ として計算するべき乗計算手段とを含む。

発明の効果

[0009] 本発明によれば、多項式の計算を行うことなく、2のべき乗の計算をすることができるため、2のべき乗の秘密計算に必要な計算時間を削減することが可能となる。

図面の簡単な説明

[0010] [図1]第一実施形態の秘密計算アルゴリズムの処理手順を示す図である。

[図2]秘密計算システム10の構成を示すブロック図である。

[図3]秘密計算装置100_iの構成を示すブロック図である。

[図4]秘密計算システム10の動作を示すフローチャートである。

発明を実施するための形態

[0011] 以下、本発明の実施の形態について、詳細に説明する。なお、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。

[0012] 後述する2のべき乗の秘密計算アルゴリズムは、既存の秘密計算上の演算の組み合わせで構築される。この秘密計算アルゴリズムが必要とする演算は、秘匿化と復元、加算、減算、乗算、小数分解、左シフトである。まず、各演算の定義、記法等について説明する。

[0013] <定義、記法等>

[秘匿化と復元]

ある値 a を暗号化や秘密分散などにより秘匿化した値のことを a の秘匿文と呼び、 $[[a]]$ と表すこととする。 a の秘匿文 $[[a]]$ が秘密分散により生成されたものである場合は、 $[[a]]$ 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ものとする。

[0014] また、 a の秘匿文 $[[a]]$ を復元して、 a を得る処理を $a \leftarrow \text{Open}([[a]])$ と表すこととする。

[0015] 秘匿化と復元の方法として、具体的には、参考非特許文献1や参考非特許文献2の手法がある。

[0016] (参考非特許文献1) Octavian Catrina, Amitabh Saxena, “Secure Computation with Fixed-Point Numbers”, Financial Cryptography 2010, LNCS60

52, pp. 35-50, 2010.

[0017] (参考非特許文献2) Mehrdad Aliasgari, Marina Blanton, Yihua Zhang, Aaron Steele, "Secure Computation on Floating Point Numbers", NDSS 2013, 2013.

[0018] 参考非特許文献1には、固定小数点や整数での演算について開示されている。また、参考非特許文献2には、浮動小数点での演算について開示されている。

[0019] [加算、減算、乗算]

加算、減算、乗算の各演算は、2つの値 a , b の秘匿文 $[[a]]$, $[[b]]$ を入力とし、それぞれ $a+b$, $a-b$, ab の計算結果である和 c_1 、差 c_2 、積 c_3 の秘匿文 $[[c_1]]$, $[[c_2]]$, $[[c_3]]$ を計算する。 $[[c_1]]$, $[[c_2]]$, $[[c_3]]$ を得る処理をそれぞれ、 $[[c_1]] \leftarrow \text{Add}([a], [b])$, $[[c_2]] \leftarrow \text{Sub}([a], [b])$, $[[c_3]] \leftarrow \text{Mul}([a], [b])$ と表すこととする。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 $[a]+[b]$, $[a]-[b]$, $[a] \times [b]$ と略記することもある。

[0020] 加算、減算、乗算の方法として、具体的には、参考非特許文献1や参考非特許文献2の手法がある。参考非特許文献1には、固定小数点や整数での演算について開示されている。また、参考非特許文献2には、浮動小数点での演算について開示されている。

[0021] [小数分解]

a の秘匿文 $[[a]]$ に対して、 a の整数部分 e と小数部分 f ($0 \leq f < 1$)の秘匿文 $[[e]]$, $[[f]]$ を計算する処理を $[[e]], [[f]] \leftarrow \text{Split}([a])$ と表すこととする。

[0022] 小数分解の方法として、具体的には、非特許文献3の手法がある。非特許文献3には、浮動小数点での演算について開示されている。また、固定小数点や整数での演算については、参考非特許文献1の固定小数点数（整数）と浮動小数点数の相互変換と非特許文献3の浮動小数点数の小数分解を組み合わせればよい。

[0023] [左シフト]

aの秘匿文[[a]]とbの秘匿文[[b]]からaをbビット左シフトした値（つまり、aを 2^b 倍した値）である左シフト値 $c(=a \times 2^b)$ の秘匿文[[c]]を計算する処理を[[c]]←[[a]]<<[[b]]と表すこととする。

[0024] 浮動小数点での演算については、指数部にシフト量($x \ll y$ のyのこと)を加算すればよい。また、固定小数点や整数での演算については、参考非特許文献1の固定小数点数（整数）と浮動小数点数の相互変換と上述の浮動小数点数の左シフトを組み合わせればよい。

[0025] <第一実施形態>

第一実施形態の秘密計算アルゴリズムの入力と出力、処理手順と第一実施形態の秘密計算アルゴリズムを実現する秘密計算システムについて、以下説明していく。

[0026] [入力と出力]

図1に示す第一実施形態の秘密計算アルゴリズムの入力と出力について説明する。

[0027] 2のべき乗を計算する値xの秘匿文[[x]]が入力となる。また、 $0 \leq r < 1$ を満たす乱数rとrの2のべき乗 2^r の秘匿文[[r]], [[2^r]]も入力する。

[0028] xの2のべき乗 2^x の秘匿文[[2^x]]が出力となる。

[0029] [処理手順]

図1に示す第一実施形態の秘密計算アルゴリズムの処理手順について説明する。その際、図1の左端の数字を用いてステップ1、ステップ2等と表現することにする。

[0030] ステップ1では、入力された秘匿文[[x]]と[[r]]から、xから乱数rを減算した結果である差 $x-r$ の秘匿文[[x]]-[[r]]を計算する。次に、秘匿文[[x]]-[[r]]から、差 $x-r$ の整数部分eと小数部分 $f(0 \leq f < 1)$ の秘匿文[[e]], [[f]]を生成する。ここで、 $x-r=e+f$ が成り立つ。

[0031] ステップ2では、ステップ1で生成した秘匿文[[f]]から、差 $x-r$ の小数部分fを復元する。

[0032] ステップ3では、ステップ2で復元した小数部分fとステップ1で生成した

秘匿文 $[[e]]$ から、 f の2のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]]$ を生成する。ここで、 $[[y]] = 2^f \ll [[e]] = [[2^{f+e}]] = [[2^{x-r}]]$ が成り立つ。

[0033] ステップ4では、入力された秘匿文 $[[2^r]]$ とステップ3で生成した秘匿文 $[[y]]$ から、 2^r と y を乗算した結果である積 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を計算する。ここで、 $[[2^r]] \times [[y]] = [[2^r \times y]] = [[2^r \times 2^{x-r}]] = [[2^x]]$ が成り立つ。

[0034] [秘密計算システム]

以下、図2～図4を参照して第一実施形態の秘密計算システム10について説明する。図2は、秘密計算システム10の構成を示すブロック図である。秘密計算システム10は、 W 個（ W は2以上の所定の整数）の秘密計算装置 100_1 、 $\dots$ 、 100_W を含む。秘密計算装置 100_1 、 $\dots$ 、 100_W は、ネットワーク800に接続しており、相互に通信可能である。ネットワーク800は、例えば、インターネットなどの通信網あるいは同報通信路などでよい。図3は、秘密計算装置 100_i （ $1 \leq i \leq W$ ）の構成を示すブロック図である。図4は、秘密計算システム10の動作を示すフローチャートである。

[0035] 図3に示すように秘密計算装置 100_i は、乱数生成部110 $_i$ と、小数分解部120 $_i$ と、復元部130 $_i$ と、左シフト部140 $_i$ と、べき乗計算部150 $_i$ と、記録部190 $_i$ を含む。記録部190 $_i$ を除く秘密計算装置 100_i の各構成部は、秘密計算アルゴリズムで必要とされる演算、つまり、少なくとも秘匿化、復元、加算、減算、乗算、小数分解、左シフトのうち、各構成部の機能を実現するうえで必要になる演算を実行できるように構成されている。本発明において個々の演算を実現するための具体的な機能構成は、例えば先行技術文献として開示している非特許文献や＜定義、記法等＞で開示している参考非特許文献などにあるアルゴリズムを実行できるような構成で十分であり、これらは従来的構成であるから詳細な説明については省略する。また、記録部190 $_i$ は、秘密計算装置 100_i の処理に必要な情報を記録する構成部である。

[0036] W 個の秘密計算装置 100_i による協調計算によって、秘密計算システム10

はマルチパーティプロトコルである秘密計算アルゴリズムを実現する。よって、秘密計算システム 10 の乱数生成手段 110（図示していない）は乱数生成部 110₁、…、110_Wで構成され、小数分解手段 120（図示していない）は小数分解部 120₁、…、120_Wで構成され、復元手段 130（図示していない）は復元部 130₁、…、130_Wで構成され、左シフト手段 140（図示していない）は左シフト部 140₁、…、140_Wで構成され、べき乗計算手段 150（図示していない）はべき乗計算部 150₁、…、150_Wで構成される。

[0037] 秘密計算システム 10 は、事前に生成した乱数 r ($0 \leq r < 1$) とその 2 のべき乗 2^r の秘匿文 $[[r]]$, $[[2^r]]$ を用いて、2 のべき乗を計算する値（つまり、指数） x の秘匿文 $[[x]]$ から、 x の 2 のべき乗 2^x の秘匿文 $[[2^x]]$ を計算する。以下、図 4 に従い秘密計算システム 10 の動作について説明する。

[0038] 乱数生成手段 110 は、 $0 \leq r < 1$ を満たす乱数 r を生成し、秘匿文 $[[r]]$, $[[2^r]]$ を生成する（S 110）。図 1 の秘密計算アルゴリズムの入力値の事前セットアップに対応する。秘匿文 $[[r]]$, $[[2^r]]$ は、記録部 190₁、…、190_W に記録しておく。

[0039] 小数分解手段 120 は、秘匿文 $[[x]]$ が入力される前に生成しておいた秘匿文 $[[r]]$ を用いて、 x の秘匿文 $[[x]]$ から、 x と乱数 r の差 $x-r$ の秘匿文 $[[x]] - [[r]]$ を計算し、秘匿文 $[[x]] - [[r]]$ から、差 $x-r$ の整数部分 e と小数部分 f ($0 \leq f < 1$) の秘匿文 $[[e]]$, $[[f]]$ を生成する（S 120）。図 1 の秘密計算アルゴリズムのステップ 1 に対応する。

[0040] 復元手段 130 は、S 120 で生成した秘匿文 $[[f]]$ から、小数部分 f を復元する（S 130）。図 1 の秘密計算アルゴリズムのステップ 2 に対応する。

[0041] 左シフト手段 140 は、S 130 で復元した小数部分 f と S 120 で生成した秘匿文 $[[e]]$ から、小数部分 f の 2 のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]] = 2^f \ll [[e]]$ を生成する（S 140）。図 1 の秘密計算アルゴリズムのステップ 3 に対応する。

[0042] べき乗計算手段150は、秘匿文 $[[x]]$ が入力される前に生成しておいた秘匿文 $[[2^r]]$ を用いて、S140で生成した秘匿文 $[[y]]$ から、2のべき乗 2^r と左シフト値 y を乗算した結果である積 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を計算する（S150）。図1の秘密計算アルゴリズムのステップ4に対応する。

[0043] 本実施形態の発明によれば、 2^x の計算を減算、小数分解、復元、左シフト、乗算をそれぞれ1回実行することで実現できるため、計算コストが削減される。また、 $[[2^r]]$ が与えられていることを前提とし、 $2^x = 2^{x-r} \times 2^r$ であることを利用し、入力値 $[[x]]$ から出力値 $[[2^x]]$ を計算する処理を $[[2^{x-r}]]$ の計算に還元している。通常、 2^{x-r} の指数 $x-r$ の小数部分 f を復元すると情報が漏れてしまうが、指数 $x-r$ の小数部分が0以上1未満の一樣ランダムな値となるように調整（つまり、 $x-r$ を計算してから小数部分を抜き出して小数部分のみを公開）することにより、安全に 2^x の計算を実行することを可能としている。

[0044] <補記>

本発明の装置は、例えば単一のハードウェアエンティティとして、キーボードなどが接続可能な入力部、液晶ディスプレイなどが接続可能な出力部、ハードウェアエンティティの外部に通信可能な通信装置（例えば通信ケーブル）が接続可能な通信部、CPU（Central Processing Unit、キャッシュメモリやレジスタなどを備えていてもよい）、メモリであるRAMやROM、ハードディスクである外部記憶装置並びにこれらの入力部、出力部、通信部、CPU、RAM、ROM、外部記憶装置の間のデータのやり取りが可能なように接続するバスを有している。また必要に応じて、ハードウェアエンティティに、CD-ROMなどの記録媒体を読み書きできる装置（ドライブ）などを設けることとしてもよい。このようなハードウェア資源を備えた物理的実体としては、汎用コンピュータなどがある。

[0045] ハードウェアエンティティの外部記憶装置には、上述の機能を実現するために必要となるプログラムおよびこのプログラムの処理において必要となるデータなどが記憶されている（外部記憶装置に限らず、例えばプログラムを読み出し専用記憶装置であるROMに記憶しておくこととしてもよい）。

また、これらのプログラムの処理によって得られるデータなどは、RAMや外部記憶装置などに適宜に記憶される。

[0046] ハードウェアエンティティでは、外部記憶装置（あるいはROMなど）に記憶された各プログラムとこの各プログラムの処理に必要なデータが必要に応じてメモリに読み込まれて、適宜にCPUで解釈実行・処理される。その結果、CPUが所定の機能（上記、…部、…手段などと表した各構成要件）を実現する。

[0047] 本発明は上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。また、上記実施形態において説明した処理は、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るとしてもよい。

[0048] 既述のように、上記実施形態において説明したハードウェアエンティティ（本発明の装置）における処理機能をコンピュータによって実現する場合、ハードウェアエンティティ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、このプログラムをコンピュータで実行することにより、上記ハードウェアエンティティにおける処理機能がコンピュータ上で実現される。

[0049] 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。具体的には、例えば、磁気記録装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、DVD（Digital Versatile Disc）、DVD-RAM（Random Access Memory）、CD-ROM（Compact Disc Read Only Memory）、CD-R（Recordable）／RW（ReWritable）等を、光磁気記録媒体として、MO（Magneto-Optical disc）等を、半導体メモリとしてEEP-ROM（Electrically Erasable and Programmable-Read Only Memory）等を用いるこ

とができる。

[0050] 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。

[0051] 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、自己の記録媒体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。

[0052] 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、ハードウェアエンティティ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。

[0053] 上述の本発明の実施形態の記載は、例証と記載の目的で提示されたものである。網羅的であるという意思はなく、開示された厳密な形式に発明を限定

する意思もない。変形やバリエーションは上述の教示から可能である。実施形態は、本発明の原理の最も良い例証を提供するために、そして、この分野の当業者が、熟考された実際の使用に適するように本発明を色々な実施形態で、また、色々な変形を付加して利用できるようにするために、選ばれて表現されたものである。すべてのそのような変形やバリエーションは、公正に合法的に公平に与えられる幅にしたがって解釈された添付の請求項によって定められた本発明のスコープ内である。

請求の範囲

- [請求項1] r を $0 \leq r < 1$ を満たす乱数、 $[[r]]$ を前記乱数 r の秘匿文、 $[[2^r]]$ を前記乱数 r の2のべき乗 2^r の秘匿文とし、
- 2個以上の秘密計算装置で構成され、2のべき乗を計算する値 x の秘匿文 $[[x]]$ から、前記値 x の2のべき乗 2^x の秘匿文 $[[2^x]]$ を計算する秘密計算システムであって、
- 前記秘匿文 $[[r]]$ を用いて、前記秘匿文 $[[x]]$ から前記値 x と前記乱数 r の差 $x-r$ の秘匿文 $[[x]]-[[r]]$ を計算し、前記秘匿文 $[[x]]-[[r]]$ から前記差 $x-r$ の整数部分 e と小数部分 f ($0 \leq f < 1$)の秘匿文 $[[e]]$, $[[f]]$ を生成する小数分解手段と、
- 前記秘匿文 $[[f]]$ から、前記小数部分 f を復元する復元手段と、
- 前記小数部分 f と前記秘匿文 $[[e]]$ から、前記小数部分 f の2のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]]$ を生成する左シフト手段と、
- 前記秘匿文 $[[2^r]]$ を用いて、前記秘匿文 $[[y]]$ から前記2のべき乗 2^r と前記左シフト値 y を乗算した値 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を前記秘匿文 $[[2^x]]$ として計算するべき乗計算手段と
- を含む秘密計算システム。
- [請求項2] r を $0 \leq r < 1$ を満たす乱数、 $[[r]]$ を前記乱数 r の秘匿文、 $[[2^r]]$ を前記乱数 r の2のべき乗 2^r の秘匿文とし、
- 2のべき乗を計算する値 x の秘匿文 $[[x]]$ から、前記値 x の2のべき乗 2^x の秘匿文 $[[2^x]]$ を計算する2個以上の秘密計算装置で構成される秘密計算システムの中の秘密計算装置であって、
- 前記秘匿文 $[[r]]$ を用いて、前記秘匿文 $[[x]]$ から前記値 x と前記乱数 r の差 $x-r$ の秘匿文 $[[x]]-[[r]]$ を計算し、前記秘匿文 $[[x]]-[[r]]$ から前記差 $x-r$ の整数部分 e と小数部分 f ($0 \leq f < 1$)の秘匿文 $[[e]]$, $[[f]]$ を生成する小数分解部と、
- 前記秘匿文 $[[f]]$ から、前記小数部分 f を復元する復元部と、

前記小数部分 f と前記秘匿文 $[[e]]$ から、前記小数部分 f の2のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]]$ を生成する左シフト部と、

前記秘匿文 $[[2^r]]$ を用いて、前記秘匿文 $[[y]]$ から前記2のべき乗 2^r と前記左シフト値 y を乗算した値 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を前記秘匿文 $[[2^x]]$ として計算するべき乗計算部と

を含む秘密計算装置。

[請求項3] r を $0 \leq r < 1$ を満たす乱数、 $[[r]]$ を前記乱数 r の秘匿文、 $[[2^r]]$ を前記乱数 r の2のべき乗 2^r の秘匿文とし、

2個以上の秘密計算装置で構成される秘密計算システムを用いて、2のべき乗を計算する値 x の秘匿文 $[[x]]$ から、前記値 x の2のべき乗 2^x の秘匿文 $[[2^x]]$ を計算する秘密計算方法であって、

前記秘密計算システムが、前記秘匿文 $[[r]]$ を用いて、前記秘匿文 $[[x]]$ から前記値 x と前記乱数 r の差 $x-r$ の秘匿文 $[[x]]-[[r]]$ を計算し、前記秘匿文 $[[x]]-[[r]]$ から前記差 $x-r$ の整数部分 e と小数部分 f ($0 \leq f < 1$)の秘匿文 $[[e]]$, $[[f]]$ を生成する小数分解ステップと、

前記秘密計算システムが、前記秘匿文 $[[f]]$ から、前記小数部分 f を復元する復元ステップと、

前記秘密計算システムが、前記小数部分 f と前記秘匿文 $[[e]]$ から、前記小数部分 f の2のべき乗 2^f を e ビット左シフトした値である左シフト値 y の秘匿文 $[[y]]$ を生成する左シフトステップと、

前記秘密計算システムが、前記秘匿文 $[[2^r]]$ を用いて、前記秘匿文 $[[y]]$ から前記2のべき乗 2^r と前記左シフト値 y を乗算した値 $2^r \times y$ の秘匿文 $[[2^r]] \times [[y]]$ を前記秘匿文 $[[2^x]]$ として計算するべき乗計算ステップと

を実行する秘密計算方法。

[請求項4] 請求項1に記載の秘密計算システムを構成する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。

[図1]

秘密計算アルゴリズム（第一実施形態）

Input: $[[x]]$, $[[r]]$, $[[2^r]]$ Output: $[[2^x]]$ 1: $[[e]], [[f]] \leftarrow \text{Split}([x] - [r])$ 2: $f \leftarrow \text{Open}([f])$ 3: $[[y]] \leftarrow 2^f \ll [e]$ 4: $[[2^x]] \leftarrow [[2^r]] \times [[y]]$

図 1

[図2]

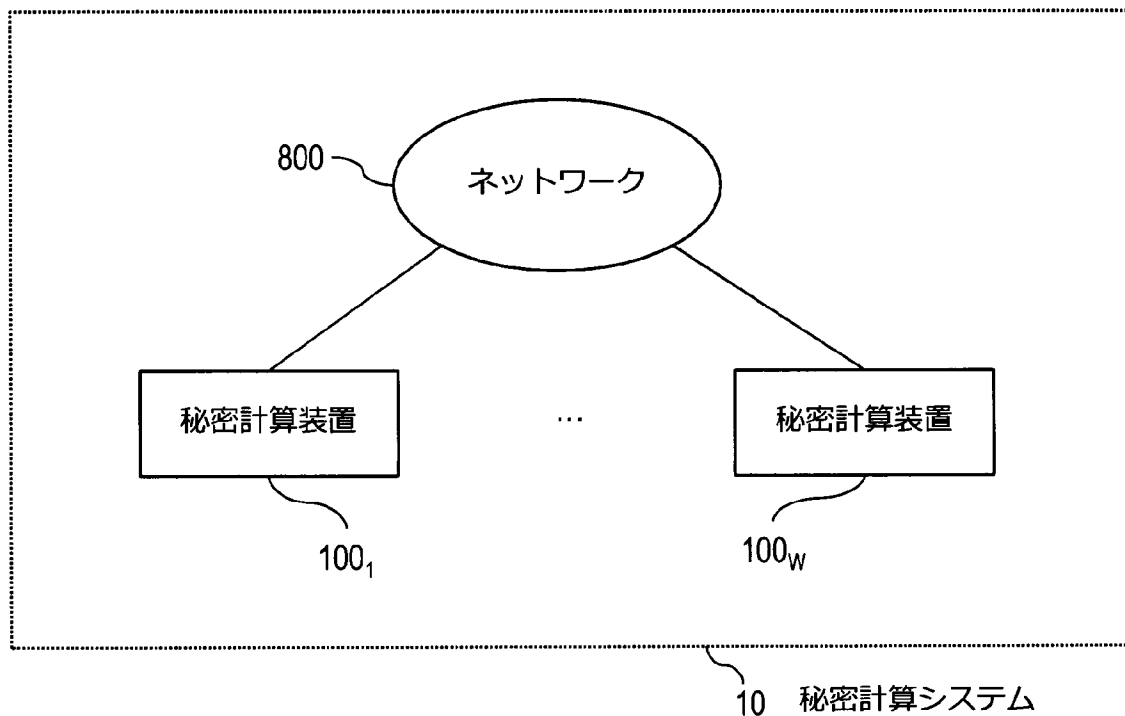


図 2

[図3]

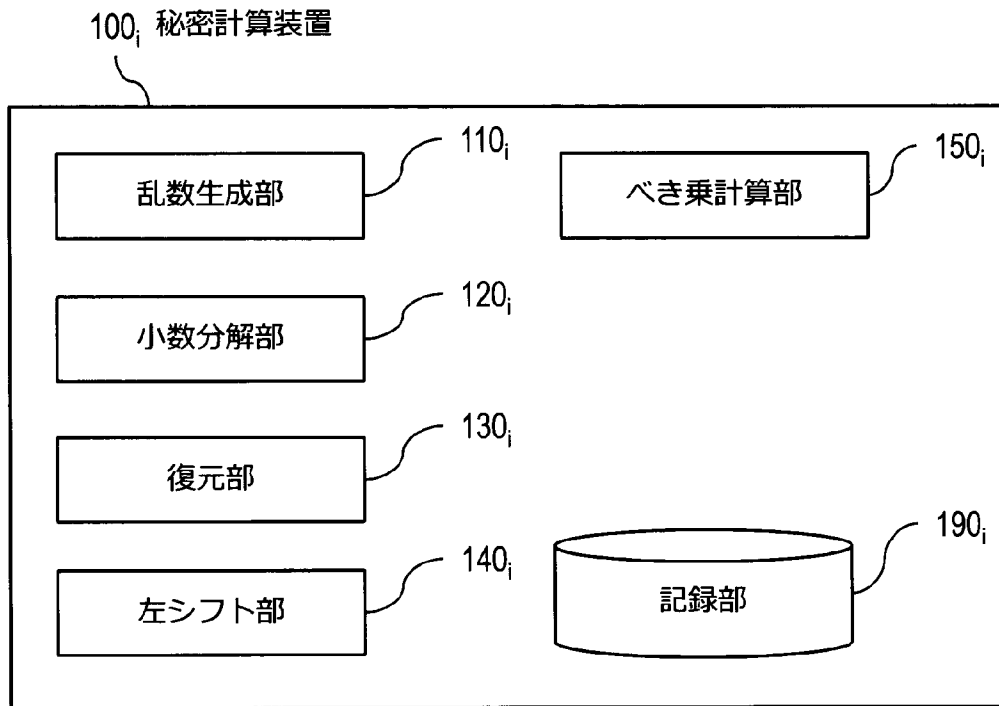


図3

[図4]

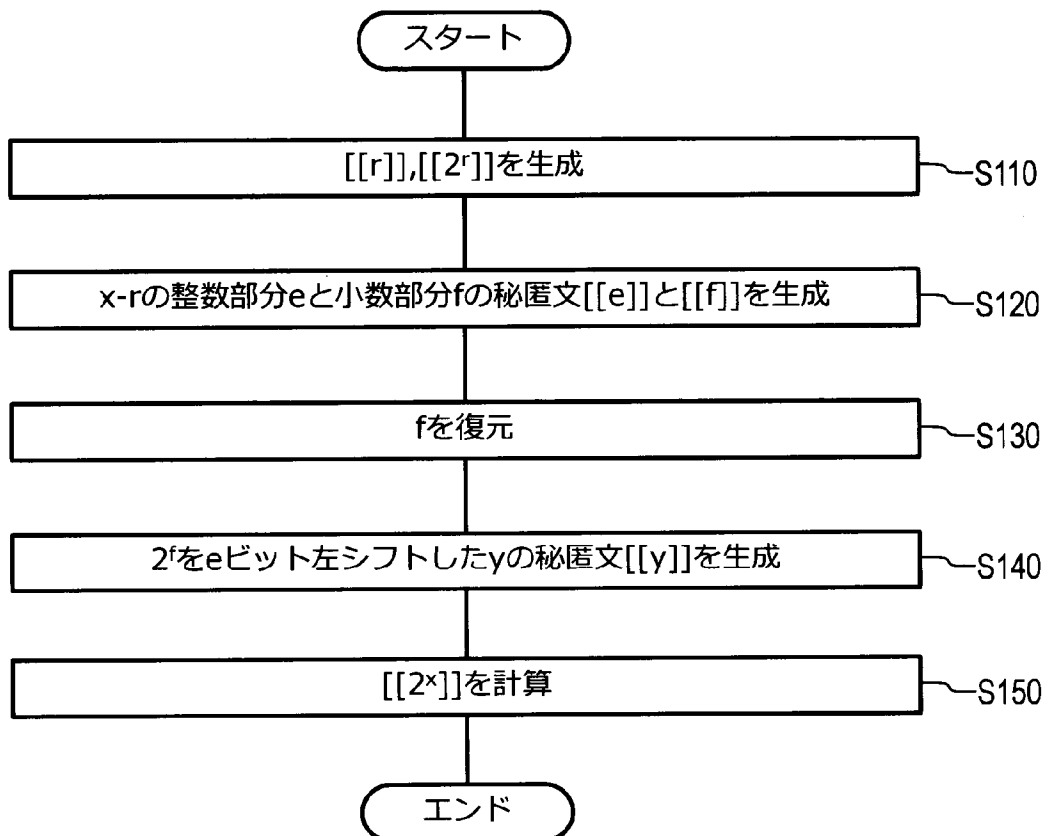


図4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/001346

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G09C1/00 (2006.01) i, G06F7/552 (2006.01) i

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)

Int.Cl. G09C1/00, G06F7/552

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2018
Registered utility model specifications of Japan	1996-2018
Published registered utility model applications of Japan	1994-2018

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAMM, L. and WILLEMSOM, J., Secure floating point arithmetic and private satellite collision analysis, International Journal of Information Security, November 2015, vol. 14, issue 6, pp. 531-548, <DOI:10.1007/s10207-014-0271-8>	1-4
A	LIU, X. M. et al., Privacy-preserving outsourced calculation on floating point numbers, IEEE Transactions on Information Forensics and Security, November 2016, vol. 11, no. 11, pp. 2513-2527, <DOI:10.1109/TIFS.2016.2585152>	1-4

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
31.01.2018

Date of mailing of the international search report
13.02.2018

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/001346

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	濱田浩気, 実行時に効率的な初等関数の秘密計算アルゴリズム, 2017 年暗号と情報セキュリティシンポジウム, 27 January 2017, 2D3-4, pp. 1-8 (HAMADA, Koki, 2017 Symposium on Cryptography and Information Security), non-official translation (Efficient secret computation algorithm of elementary functions during operation hours)	1-4

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. G09C1/00(2006.01)i, G06F7/552(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. G09C1/00, G06F7/552

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2018年
日本国実用新案登録公報	1996-2018年
日本国登録実用新案公報	1994-2018年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	KAMM, Liina and WILLEMSOM, Jan, Secure floating point arithmetic and private satellite collision analysis, International Journal of Information Security, 2015.11, Volume 14, Issue 6, pp. 531-548, <DOI: 10.1007/s10207-014-0271-8>	1-4
A	LIU, Ximeng et al., Privacy-Preserving Outsourced Calculation on Floating Point Numbers, IEEE Transactions on Information Forensics and Security, 2016.11, Vol. 11, No. 11, pp. 2513-2527, <DOI: 10.1109/TIFS.2016.2585152>	1-4

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- | | |
|--|---|
| 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの | 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの |
| 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの | 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの |
| 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) | 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの |
| 「O」 口頭による開示、使用、展示等に言及する文献 | 「&」 同一パテントファミリー文献 |
| 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 | |

国際調査を完了した日

31.01.2018

国際調査報告の発送日

13.02.2018

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

金沢 史明

5 S

4538

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
P, X	濱田浩気, 実行時に効率的な初等関数の秘密計算アルゴリズム, 2017 年暗号と情報セキュリティシンポジウム, 2017.01.27, 2D3-4, pp. 1-8	1-4