(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
2005 年8 月4 日 (04.08.2005)

PCT

(10) 国際公開番号
WO 2005/071640 A1

(51) 国際特許分類[7]: G09C 1/00

(21) 国際出願番号: PCT/JP2005/001437

(22) 国際出願日: 2005 年1 月26 日 (26.01.2005)

(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2004-016881 2004 年1 月26 日 (26.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 古川 潤 (FURUKAWA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 寺西 勇 (TERANISHI, Isamu) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

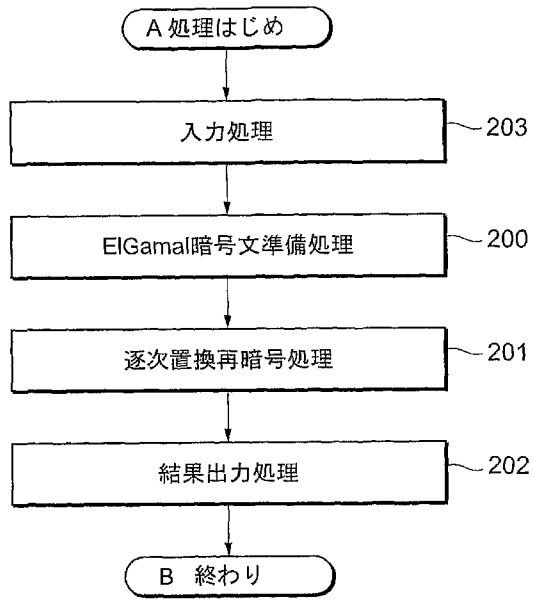
(74) 代理人: 池田 憲保 (IKEDA, Noriyasu); 〒1050003 東京都港区西新橋一丁目４番１０号 第３森ビル Tokyo (JP).

(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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,

[続葉有]

(54) Title: METHOD AND DEVICE FOR CALCULATING A FUNCTION FROM A PLENTY OF INPUTS

(54) 発明の名称: 多数の入力から関数を計算する方法および装置



A PROCESS START
203 INPUT PROCESS
200 E|Gama| ENCRYPTED SENTENCE PREPARATION PROCESS
201 SUCCESSIVE REPLACEMENT RE-ENCRYPTION PROCESS
202 RESULT OUTPUT PROCESS
B END

(57) Abstract: In an input process, a circuit and an input bit to the circuit are inputted to a plurality of computers. Firstly, one of the computers performs calculation and transmits the calculation result to another computer. Next, the another computer which has received the calculation result performs the next calculation. Thus, calculation is performed by one computer after another. When all the computers have performed calculation once, the last computer which has performed calculation transmits the calculation result to the first computer which has performed calculation. After this, calculation is performed by one computer after another and the calculation result is transmitted to the next computer, thereby repeating the calculation of each cycle. Thus, it is possible to realize calculation of a value of a given function by using a device including a plurality of computers, with a more simple configuration.

(57) 要約: 入力処理では、複数の計算装置に、回路と、回路への入力ビットとが入力され、まず一台の計算装置が計算を行い、その計算結果を他の計算装置のうち一台に送り、次にその計算結果を受け取った前記計算装置がその次の計算を行う、というとようにに一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする。これにより、複数の計算装置を含む機器を用いて与えられた関数の値を計算することをより簡単な構成で実現する。

WO 2005/071640 A1

LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領 の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。