

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第2区分

【発行日】令和4年8月19日(2022.8.19)

【国際公開番号】WO2021/149106

【出願番号】特願2021-572128(P2021-572128)

【国際特許分類】

G 0 9 C 1 / 0 0 ( 2 0 0 6 . 0 1 )

【 F I 】

G 0 9 C 1 / 0 0 6 5 0 Z

10

【手続補正書】

【提出日】令和4年6月23日(2022.6.23)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0033

【補正方法】変更

【補正の内容】

【0033】

図3は、実施形態における秘密計算装置1のハードウェア構成を例示したブロック図である。図3に例示するように、この例の秘密計算装置1は、CPU(Central Processing Unit)10a、入力部10b、出力部10c、RAM(Random Access Memory)10d、ROM(Read Only Memory)10e、補助記憶装置10f及びバス10gを有している。この例のCPU10aは、制御部10aa、演算部10ab及びレジスタ10acを有し、レジスタ10acに読み込まれた各種プログラムに従って様々な演算処理を実行する。また、出力部10cは、データが出力される出力端子、ディスプレイ等、所定のプログラムを読み込んだCPU10aによって制御されるLANカード等である。また、RAM10dは、SRAM(Static Random Access Memory)、DRAM(Dynamic Random Access Memory)等であり、所定のプログラムが格納されるプログラム領域10da及び各種データが格納されるデータ領域10dbを有している。また、補助記憶装置10fは、例えば、ハードディスク、MO(Magneto-Optical disc)、半導体メモリ等であり、所定のプログラムが格納されるプログラム領域10fa及び各種データが格納されるデータ領域10fbを有している。また、バス10gは、CPU10a、入力部10b、出力部10c、RAM10d、ROM10e及び補助記憶装置10fを、情報のやり取りが可能ないように接続する。CPU10aは、読み込まれたOS(Operating System)プログラムに従い、補助記憶装置10fのプログラム領域10faに格納されているプログラムをRAM10dのプログラム領域10daに書き込む。同様にCPU10aは、補助記憶装置10fのデータ領域10fbに格納されている各種データを、RAM10dのデータ領域10dbに書き込む。そして、このプログラムやデータが書き込まれたRAM10d上のアドレスがCPU10aのレジスタ10acに格納される。CPU10aの制御部10abは、レジスタ10acに格納されたこれらのアドレスを順次読み出し、読み出したアドレスが示すRAM10d上の領域からプログラムやデータを読み出し、そのプログラムが示す演算を演算部10abに順次実行させ、その演算結果をレジスタ10acに格納していく。このような構成により、図1Aに例示した秘密計算装置1の機能構成が実現される。

20

30

40