【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】WO2021/149105
【出願番号】特願2021-572127(P2021-572127)
【国際特許分類】
Ｇ０９Ｃ　1/00(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６５０Ｚ

【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】００２９
【補正方法】変更
【補正の内容】
【００２９】
図６は、実施形態における秘密計算装置１，２のハードウェア構成を例示したブロック図である。図６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、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、秘密計算装置１，２の機能構成が実現される。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図２
【補正方法】変更
【補正の内容】

【図２】

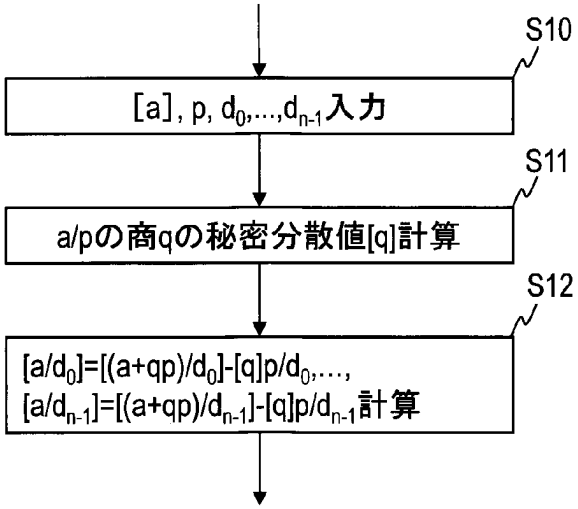

S10
[a], p, d_0,...,d_{n-1}入力
S11
a/pの商qの秘密分散値[q]計算
S12
[a/d_0]=[(a+qp)/d_0]-[q]p/d_0,...,
[a/d_{n-1}]=[(a+qp)/d_{n-1}]-[q]p/d_{n-1}計算

図２