【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７部門第３区分
【発行日】令和2年4月16日(2020.4.16)

【公表番号】特表2020-500458(P2020-500458A)
【公表日】令和2年1月9日(2020.1.9)
【年通号数】公開・登録公報2020-001
【出願番号】特願2019-521112(P2019-521112)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ

【手続補正書】
【提出日】令和2年3月4日(2020.3.4)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００５２
【補正方法】変更
【補正の内容】
【００５２】
入力値のＰｅｄｅｒｓｅｎコミットメントは、第１ジェネレータＧとの関係において第２ジェネレータＨの離散対数（或いは、逆もまた然り）をだれも知らないように、グループの更なるジェネレータ（以下の式におけるＨ）を選ぶことにより、生成することができるが、これは、ｘＧ＝Ｈとなるようなｘをだれも知らないことを意味している。これは、例えば、Ｇの暗号学的ハッシュを使用してＨを選択することにより、実現されてもよく、即ち、Ｈ＝ｔｏ＿ｐｏｉｎｔ（ＳＨＡ２５６（ＥＮＣＯＤＥ（Ｇ））である。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００９１
【補正方法】変更
【補正の内容】
【００９１】
メインメモリ５０６、ＲＯＭ５０８、及び／又はストレージ装置５１０は、一時的ではないストレージ媒体を含むことができる。本明細書において使用されている「一時的ではない媒体」という用語及び類似の用語は、機械が特定の方式において動作するようにするデータ及び／又は命令を保存する媒体を意味しており、媒体は、一時的な信号を除外している。このような一時的ではない媒体は、不揮発性媒体及び／又は揮発性媒体を有することができる。不揮発性媒体は、例えば、ストレージ装置５１０などの、光又は磁気ディスクを含む。揮発性媒体は、メインメモリ５０６などの、ダイナミックメモリを含む。一時的ではない媒体の一般的な形態は、例えば、フロッピーディスク、フレキシブルディスク、ハードディスク、半導体ドライブ、磁気テープ、又は任意のその他の磁気データストレージ媒体、ＣＤ－ＲＯＭ、任意のその他の光データストレージ媒体、孔のパターンを有する任意の物理的媒体、ＲＡＭ、ＰＲＯＭ、及びＥＰＲＯＭ、ＦＬＡＳＨ－ＥＰＲＯＭ、ＮＶＲＡＭ、任意のその他のメモリチップ又はカートリッジ、及びこれらのもののネットワーク接続されたバージョンを含む。