【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2020-507222(P2020-507222A)
【公表日】令和2年3月5日(2020.3.5)
【年通号数】公開・登録公報2020-009
【出願番号】特願2019-520853(P2019-520853)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/38　(2012.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｚ
Ｇ０６Ｑ　20/38　３１０
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】令和2年2月13日(2020.2.13)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】変更
【補正の内容】
【００５３】
入力値に対するペダーソンコミットメントを、ｘＧ＝Ｈとなるようなｘを誰も知らないことを意味する第１の生成元Ｇに対する第２の生成元Ｈの離散対数（逆の場合も同じ）を誰も知らないようにするように群（下の式のＨ）の他の生成元を取り出すことによって作成してもよい。これを、例えば、Ｈ：　Ｈ＝ｔｏ＿ｐｏｉｎｔ（ＳＨＡ２５６（ＥＮＣＯＤＥ（Ｇ））））を取り出すためにＧの暗号化ハッシュを用いることによって成し遂げてもよい。