【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3年7月26日(2021.7.26)

【公表番号】特表2020-526055(P2020-526055A)
【公表日】令和2年8月27日(2020.8.27)
【年通号数】公開・登録公報2020-034
【出願番号】特願2019-561993(P2019-561993)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　21/64
Ｇ０６Ｆ　21/62　３１８

【手続補正書】
【提出日】令和3年5月10日(2021.5.10)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
第１ノードが第２ノードとの信頼できる通信を確立するための、コンピュータにより実施される方法であって、前記第２ノードが第２ノード識別子及び第２シークレットポイントを有し、前記第２シークレットポイントが、グループ秘密鍵に前記第２ノード識別子のマップ・ツー・ポイントハッシュを掛けたものであり、前記グループ秘密鍵が、クレデンシャルを付与するよう構成されたノードのグループに関連する、前記方法において、
前記グループ秘密鍵に第１ノード識別子のマップ・ツー・ポイントハッシュを掛けたものである第１シークレットポイントを前記ノードのグループから得ることと、
前記第１ノード識別子を前記第２ノードへ送ることと、
前記第２ノード識別子を受け取ることと、
前記第２ノード識別子のマップ・ツー・ポイントハッシュと、前記第１シークレットポイントとによる双線形ペアリング操作を用いて、第１セッション鍵を生成することと、
前記第１セッション鍵が、前記第２ノードによって、前記第２シークレットポイントと、前記第１ノード識別子のマップ・ツー・ポイントハッシュとによる前記双線形ペアリング操作を用いて生成された第２セッション鍵と一致することを確かめることと
を有する方法。
【請求項２】
前記第１セッション鍵を生成するための前記双線形ペアリング操作は、式：

$$K_A = e(H_1(id_B), s_A)$$、及び

$$K_A = e(s_B, H_1(id_A))$$

のうちの一方を有し、前記第２セッション鍵を生成するための前記双線形ペアリング操作は、前記式のうちの他方を有し、
ｅ（）は、前記双線形ペアリング操作であり、
H_1（）は、前記マップ・ツー・ポイントハッシュであり、
id_A及びid_Bは、前記第１ノード識別子及び前記第２ノード識別子の夫々１つであり、
s_A及びs_Bは、前記第１シークレットポイント及び前記第２シークレットポイントの夫々１つである、
請求項１に記載の方法。
【請求項３】
前記第１シークレットポイントを得ることは、前記ノードのグループ内の複数のノードの夫々から前記第１シークレットポイントの各々の部分を取得し、該各々の部分を結合して、前記グループ秘密鍵を再構成することなしに前記第１シークレットポイントを形成することを有する、
請求項１又は２に記載の方法。
【請求項４】
前記確かめることは、前記第１セッション鍵により暗号化された課題を前記第１ノードから前記第２ノードへ送り、該課題に対する応答を受け取り、該応答に基づき、前記第２ノードが前記第２セッション鍵を用いて前記課題を有効に暗号解読したことを決定することを有する、
請求項１乃至３のうちいずれか一項に記載の方法。
【請求項５】
前記送ることは、第１ノンスを送ることを更に含み、
前記受け取ることは、第２ノンスと、計算されたC_0値とを受け取ることを更に含み、
前記C_0値は、前記第２セッション鍵、前記第１ノンス、及び前記第２ノンスの連結のハッシュを有する、
請求項１乃至３のうちいずれか一項に記載の方法。
【請求項６】
前記連結は、前記第１ノード識別子及び前記第２ノード識別子を更に含む、
請求項５に記載の方法。
【請求項７】
前記生成することは、前記第１セッション鍵、前記第１ノンス、及び前記第２ノンスの連結のハッシュを有する計算されたC_1値を生成することを含み、
前記確かめることは、前記計算されたC_0値が前記計算されたC_1値と一致することを確かめることを有する、
請求項５又は６に記載の方法。
【請求項８】
前記第２シークレットポイントは、前記グループ秘密鍵に前記第２ノード識別子のマップ・ツー・ポイントハッシュを掛けたものである、
請求項１乃至７のうちいずれか一項に記載の方法。
【請求項９】
前記第１シークレットポイント及び前記第２シークレットポイントは、夫々が、前記ノードのグループによって、秘密分散を用いて夫々前記第１ノード及び前記第２ノードへ供給される、
請求項１乃至８のうちいずれか一項に記載の方法。
【請求項１０】
プロセッサと、
メモリと、
ネットワークインターフェイスと、
第２ノードとの信頼できる通信を確立するためのプロセッサ実行可能命令を含み、前記

第２ノードが第２ノード識別子及び第２シークレットポイントを有し、前記第２シークレットポイントが、グループ秘密鍵に前記第２ノード識別子のマップ・ツー・ポイントハッシュを掛けたものであり、前記グループ秘密鍵が、クレデンシャルを付与するよう構成されたノードのグループに関連する、ブロックチェーンアプリケーションと
を有する第１ノードであって、
実行されるときに、前記プロセッサ実行可能命令は、当該第１ノードに、
前記グループ秘密鍵に第１ノード識別子のマップ・ツー・ポイントハッシュを掛けたものである第１シークレットポイントを前記ノードのグループから得ることと、
前記第１ノード識別子を前記第２ノードへ送ることと、
前記第２ノード識別子を受け取ることと、
前記第２ノード識別子のマップ・ツー・ポイントハッシュと、前記第１シークレットポイントとによる双線形ペアリング操作を用いて、第１セッション鍵を生成することと、
前記第１セッション鍵が、前記第２ノードによって、前記第２シークレットポイントと、前記第１ノード識別子のマップ・ツー・ポイントハッシュとによる前記双線形ペアリング操作を用いて生成された第２セッション鍵と一致することを確かめることと
を実行させる、第１ノード。
【請求項１１】
前記第１セッション鍵を生成するための前記双線形ペアリング操作は、式：

$K_A = e(H_1(id_B), s_A)$、及び

$K_A = e(s_B, H_1(id_A))$

のうちの一方を有し、前記第２セッション鍵を生成するための前記双線形ペアリング操作は、前記式のうちの他方を有し、
ｅ（）は、前記双線形ペアリング操作であり、
H_1（）は、前記マップ・ツー・ポイントハッシュであり、
id_A及びid_Bは、前記第１ノード識別子及び前記第２ノード識別子の夫々１つであり、
s_A及びs_Bは、前記第１シークレットポイント及び前記第２シークレットポイントの夫々１つである、
請求項１０に記載の第１ノード。
【請求項１２】
前記プロセッサ実行可能命令は、実行されるときに、当該第１ノードに、
前記ノードのグループ内の複数のノードの夫々から前記第１シークレットポイントの各々の部分を取得し、該各々の部分を結合して、前記グループ秘密鍵を再構成することなしに前記第１シークレットポイントを形成することによって、前記第１シークレットポイントを得ることを実行させる、
請求項１０又は１１に記載の第１ノード。
【請求項１３】
前記プロセッサ実行可能命令は、実行されるときに、当該第１ノードに、
前記第１セッション鍵により暗号化された課題を前記第１ノードから前記第２ノードへ送り、該課題に対する応答を受け取り、該応答に基づき、前記第２ノードが前記第２セッション鍵を用いて前記課題を有効に暗号解読したことを決定することによって、前記確かめることを実行させる、
請求項１０乃至１２のうちいずれか一項に記載の第１ノード。
【請求項１４】
前記プロセッサ実行可能命令は、実行されるときに、当該第１ノードに、
第１ノンスを更に送ることによって前記送ることを実行させるとともに、第２ノンスと、計算されたC_0値とを更に受け取ることによって前記受け取ることを実行させ、

前記C_0値は、前記第２セッション鍵、前記第１ノンス、及び前記第２ノンスの連結のハッシュを有する、
請求項１０乃至１２のうちいずれか一項に記載の第１ノード。
【請求項１５】
前記連結は、前記第１ノード識別子及び前記第２ノード識別子を更に含む、
請求項１４に記載の第１ノード。
【請求項１６】
前記プロセッサ実行可能命令は、実行されるときに、当該第１ノードに、
前記第１セッション鍵、前記第１ノンス、及び前記第２ノンスの連結のハッシュを有する計算されたC_1値を生成することによって前記生成することを実行させるとともに、前記計算されたC_0値が前記計算されたC_1値と一致することを確かめることによって前記確かめることを実行させる、
請求項１４又は１５に記載の第１ノード。
【請求項１７】
前記第２シークレットポイントは、前記グループ秘密鍵に前記第２ノード識別子のマップ・ツー・ポイントハッシュを掛けたものである、
請求項１０乃至１６のうちいずれか一項に記載の第１ノード。
【請求項１８】
前記第１シークレットポイント及び前記第２シークレットポイントは、夫々が、前記ノードのグループによって、秘密分散を用いて夫々前記第１ノード及び前記第２ノードへ供給される、
請求項１０乃至１７のうちいずれか一項に記載の第１ノード。
【請求項１９】
１つ以上のプロセッサによって実行されるときに、該１つ以上のプロセッサに、請求項１乃至９のうちいずれか一項に記載の方法の動作を実行させるプロセッサ実行可能命令を含むプログラム。