【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4年3月30日(2022.3.30)

【国際公開番号】WO2021/009860
【出願番号】特願2021-532612(P2021-532612)
【国際特許分類】
H04L 9/32(2006.01)
G09C 1/00(2006.01)
【ＦＩ】
H04L 9/32 ２００Ｂ
G09C 1/00 ６２０Ｚ

【手続補正書】
【提出日】令和4年1月13日(2022.1.13)
【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】
データごとに異なる疑似乱数を生成し、前記生成された疑似乱数をデータと共に暗号化する暗号化手段と、
前記暗号化手段が各データの暗号化に利用した疑似乱数を再現し、前記再現された疑似乱数から前記データの正当性を証明する制御情報を生成する署名手段と、
前記データの暗号文を復号して得られた疑似乱数に基づき前記制御情報を検証し、前記制御情報の検証に成功した場合に、前記暗号文を復号して得られたデータの関数値を計算する安全実行手段と、
を含む暗号システム。
【請求項２】
前記署名手段は、前記データの関数値を得るための関数プログラムと前記再現された疑似乱数に基づき署名を計算し、前記計算された署名を前記制御情報として扱い、
前記安全実行手段は、前記計算された署名を検証する、請求項１に記載の暗号システム。
【請求項３】
前記暗号化手段が前記疑似乱数を生成するための乱数シードを生成すると共に、前記生成された乱数シードを前記暗号化手段に配布する、乱数シード管理手段をさらに含み、
前記暗号化手段は、前記配布された乱数シードを用いて前記データごとに異なる疑似乱数を生成する、請求項２に記載の暗号システム。
【請求項４】
検証鍵と署名鍵からなる署名鍵ペアと、暗号化鍵と復号鍵からなる暗号鍵ペアと、を生成する、鍵管理手段をさらに含み、
前記鍵管理手段は、前記署名鍵を前記署名手段に送信し、前記復号鍵及び前記検証鍵を前記安全実行手段に送信する、請求項３に記載の暗号システム。
【請求項５】
前記署名手段は、前記署名鍵を使って前記制御情報を生成する、請求項４に記載の暗号システム。
【請求項６】
前記安全実行手段は、前記復号鍵を用いて前記データの暗号文を復号し、前記検証鍵を用いて前記制御情報の検証を行う、請求項４又は５に記載の暗号システム。

【請求項７】
外部から前記関数プログラムと、前記関数プログラムに入力するデータの索引と前記関数プログラムに入力するデータに対応するユーザの索引を対応付けた索引ペアと、を取得すると共に、前記取得した関数プログラムと索引ペアを前記署名手段に送信する、復号手段をさらに含み、
前記署名手段は、前記索引ペアに基づき前記疑似乱数を再現するための乱数シードを前記乱数シード管理手段から取得すると共に、前記取得した関数プログラムと乱数シードに基づき前記署名を計算し、前記計算された署名を前記復号手段に送信し、
前記復号手段は、前記受信した署名を前記安全実行手段に送信する、請求項６に記載の暗号システム。
【請求項８】
前記安全実行手段は、ハードウェア支援型のメモリ暗号化機能を利用して前記関数値を計算する、請求項１乃至７のいずれか一項に記載の暗号システム。
【請求項９】
前記安全実行手段は、関数型暗号を実行する、請求項１乃至８のいずれか一つに記載の暗号システム。
【請求項１０】
前記署名手段は、ＥＣＤＳＡ（Elliptic Curve Digital Signature Algorithm）署名を生成する、請求項１乃至９のいずれか一つに記載の暗号システム。
【請求項１１】
データごとに異なる疑似乱数を生成し、前記生成された疑似乱数をデータと共に暗号化するステップと、
前記データの暗号化に利用された疑似乱数を再現し、前記再現された疑似乱数から前記データの正当性を証明する制御情報を生成するステップと、
前記データの暗号文を復号して得られた疑似乱数に基づき前記制御情報を検証し、前記制御情報の検証に成功した場合に、前記暗号文を復号して得られたデータの関数値を計算するステップと、
を含む関数値計算方法。
【請求項１２】
コンピュータに、
データごとに異なる疑似乱数を生成し、前記生成された疑似乱数をデータと共に暗号化する処理と、
前記データの暗号化に利用された疑似乱数を再現し、前記再現された疑似乱数から前記データの正当性を証明する制御情報を生成する処理と、
前記データの暗号文を復号して得られた疑似乱数に基づき前記制御情報を検証し、前記制御情報の検証に成功した場合に、前記暗号文を復号して得られたデータの関数値を計算する処理と、
を実行させるプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】
図１に示す暗号システムでは、ユーザ（暗号化装置１０）に対し乱数シードが配付される。ユーザは配付された乱数シードを利用して疑似乱数を作成し、データと共に暗号化する。署名装置２０は、ユーザに配付された乱数シードを利用してユーザがデータと共に暗号化した疑似乱数を再現し、再現した疑似乱数を利用して制御情報を作成する。安全実行装置３０は、安全な実行環境内で暗号文を復号してデータと疑似乱数を得て、疑似乱数を利用して制御情報を検証する。安全実行装置３０は、当該検証に成功すれば復号して得たデ

ータを入力とする関数値を計算する。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００９７
【補正方法】変更
【補正の内容】
【００９７】
ハッシュ値計算部１６６は、疑似乱数のリストｌ＿ｒの各要素を結合する。上記リストｌ＿ｒの各要素の結合は、
ｒ＿（ｉ１、ｊ１）｜｜ｒ＿（ｉ２、ｊ２）｜｜．．．｜｜ｒ＿（ｉｋ、ｊｋ）
となる。
ハッシュ値計算部１６６は、上記リストｌ＿ｒの各要素の結合のハッシュ値ｇを計算する（ステップＥ１５）。ハッシュ値ｇは、
ハッシュ値ｇ＝Ｇ（ｒ＿（ｉ１、ｊ１）｜｜ｒ＿（ｉ２、ｊ２）｜｜．．．｜｜ｒ＿（ｉｋ、ｊｋ））
となる。ここで、ハッシュ関数Ｇとハッシュ関数Ｈとは同じであってもよいし異なっていてもよい。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０１２３
【補正方法】変更
【補正の内容】
【０１２３】
上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。
［付記１］
データごとに異なる疑似乱数を生成し、前記生成された疑似乱数をデータと共に暗号化する暗号化装置（１０、１２０）と、
前記暗号化装置（１０、１２０）が各データの暗号化に利用した疑似乱数を再現し、前記再現された疑似乱数から前記データの正当性を証明する制御情報を生成する署名装置（２０、１６０）と、
前記データの暗号文を復号して得られた疑似乱数に基づき前記制御情報を検証し、前記制御情報の検証に成功した場合に、前記暗号文を復号して得られたデータの関数値を計算する安全実行装置（３０、１７０）と、
を含む暗号システム。
［付記２］
前記署名装置（２０、１６０）は、前記データの関数値を得るための関数プログラムと前記再現された疑似乱数に基づき署名を計算し、前記計算された署名を前記制御情報として扱い、
前記安全実行装置（３０、１７０）は、前記計算された署名を検証する、付記１に記載の暗号システム。
［付記３］
前記暗号化装置（１０、１２０）が前記疑似乱数を生成するための乱数シードを生成すると共に、前記生成された乱数シードを前記暗号化装置（１０、１２０）に配布する、乱数シード管理装置（１３０）をさらに含み、
前記暗号化装置（１０、１２０）は、前記配布された乱数シードを用いて前記データごとに異なる疑似乱数を生成する、付記２に記載の暗号システム。
［付記４］
検証鍵と署名鍵からなる署名鍵ペアと、暗号化鍵と復号鍵からなる暗号鍵ペアと、を生成する、鍵管理装置（１１０）をさらに含み、

前記鍵管理装置（１１０）は、前記署名鍵を前記署名装置（２０、１６０）に送信し、前記復号鍵及び前記検証鍵を前記安全実行装置（３０、１７０）に送信する、付記３に記載の暗号システム。
［付記５］
前記署名装置（２０、１６０）は、前記署名鍵を使って前記制御情報を生成する、付記４に記載の暗号システム。
［付記６］
前記安全実行装置（３０、１７０）は、前記復号鍵を用いて前記データの暗号文を復号し、前記検証鍵を用いて前記制御情報の検証を行う、付記４又は５に記載の暗号システム。
［付記７］
外部から前記関数プログラムと、前記関数プログラムに入力するデータの索引と前記関数プログラムに入力するデータに対応するユーザの索引を対応付けた索引ペアと、を取得すると共に、前記取得した関数プログラムと索引ペアを前記署名装置（２０、１６０）に送信する、復号装置（１５０）をさらに含み、
前記署名装置（２０、１６０）は、前記索引ペアに基づき前記疑似乱数を再現するための乱数シードを前記乱数シード管理装置（１３０）から取得すると共に、前記取得した関数プログラムと乱数シードに基づき前記署名を計算し、前記計算された署名を前記復号装置（１５０）に送信し、
前記復号装置（１５０）は、前記受信した署名を前記安全実行装置（３０、１７０）に送信する、付記６に記載の暗号システム。
［付記８］
前記安全実行装置（３０、１７０）は、ハードウェア支援型のメモリ暗号化機能を利用して前記関数値を計算する、付記１乃至７のいずれか一つに記載の暗号システム。
［付記９］
前記安全実行装置（３０、１７０）は、関数型暗号を実行する、付記１乃至８のいずれか一つに記載の暗号システム。
［付記１０］
前記署名装置（２０、１６０）は、ＥＣＤＳＡ（Elliptic Curve Digital Signature Algorithm）署名を生成する、付記１乃至９のいずれか一つに記載の暗号システム。
［付記１１］
データごとに異なる疑似乱数を生成し、前記生成された疑似乱数をデータと共に暗号化するステップと、
前記データの暗号化に利用された疑似乱数を再現し、前記再現された疑似乱数から前記データの正当性を証明する制御情報を生成するステップと、
前記データの暗号文を復号して得られた疑似乱数に基づき前記制御情報を検証し、前記制御情報の検証に成功した場合に、前記暗号文を復号して得られたデータの関数値を計算するステップと、
を含む関数値計算方法。
［付記１２］
コンピュータ（３１１）に、
データごとに異なる疑似乱数を生成し、前記生成された疑似乱数をデータと共に暗号化する処理と、
前記データの暗号化に利用された疑似乱数を再現し、前記再現された疑似乱数から前記データの正当性を証明する制御情報を生成する処理と、
前記データの暗号文を復号して得られた疑似乱数に基づき前記制御情報を検証し、前記制御情報の検証に成功した場合に、前記暗号文を復号して得られたデータの関数値を計算する処理と、
を実行させるプログラム。
なお、付記１１の形態及び付記１２の形態は、付記１の形態と同様に、付記２の形態～付記１０の形態に展開することが可能である。

【手続補正５】
【補正対象書類名】図面
【補正対象項目名】図５
【補正方法】変更
【補正の内容】
【図５】

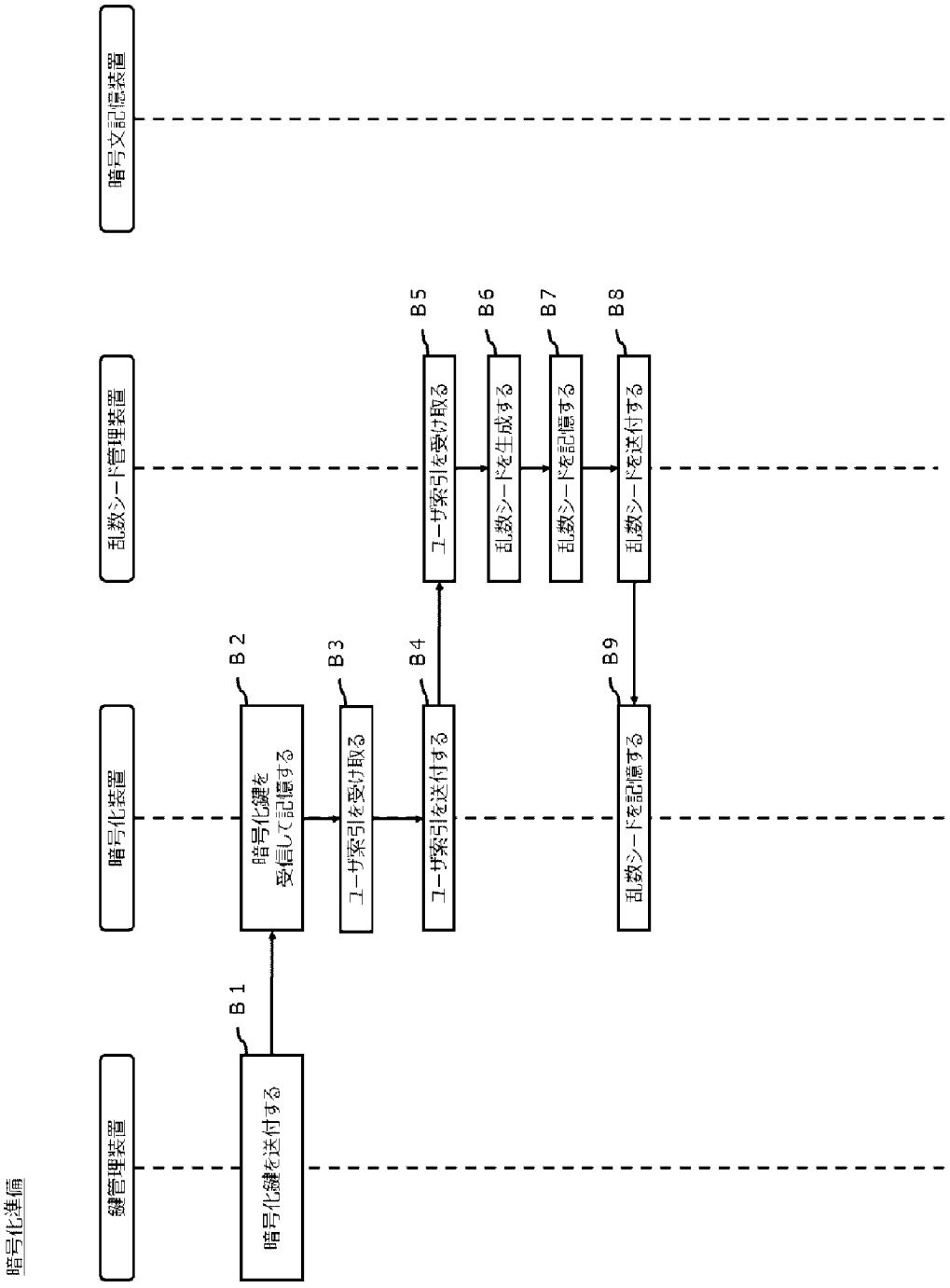

Fig.5

【手続補正６】
【補正対象書類名】図面
【補正対象項目名】図８
【補正方法】変更
【補正の内容】

【図８】

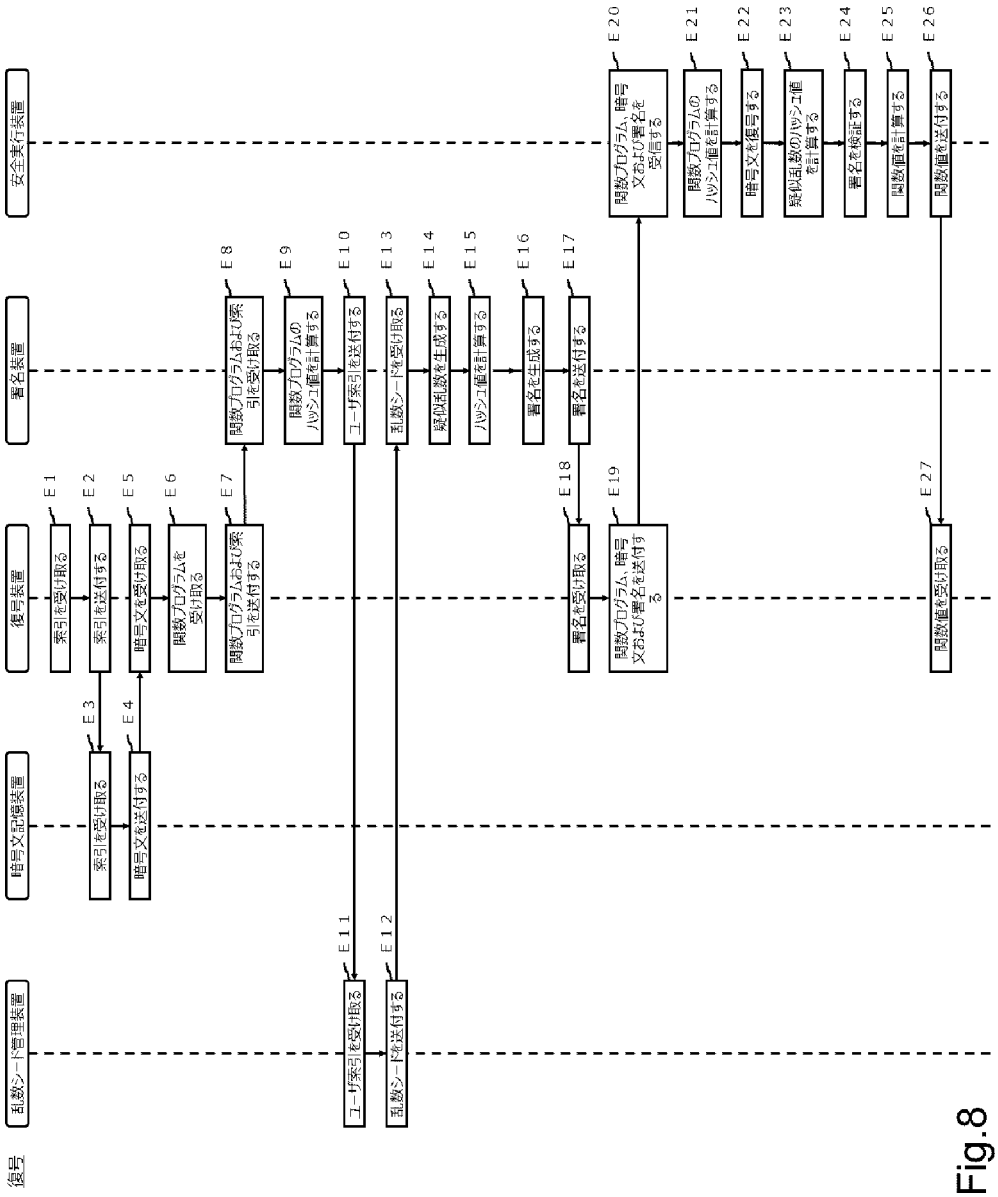
復号
乱数シード管理装置
暗号文記憶装置
復号装置
署名装置
安全実行装置
E1 索引を受け取る
E2 索引を送付する
E3 索引を受け取る
E4 暗号文を送付する
E5 暗号文を受け取る
E6 関数プログラムを受け取る
E7 関数プログラムおよび索引を送付する
E8 関数プログラムおよび索引を受け取る
E9 関数プログラムのハッシュ値を計算する
E10 ユーザ索引を送付する
E11 ユーザ索引を受け取る
E12 乱数シードを送付する
E13 乱数シードを受け取る
E14 疑似乱数を生成する
E15 ハッシュ値を計算する
E16 署名を生成する
E17 署名を送付する
E18 署名を受け取る
E19 関数プログラム、暗号文および署名を送付する
E20 関数プログラム、暗号文および署名を受信する
E21 関数プログラムのハッシュ値を計算する
E22 暗号文を復号する
E23 疑似乱数のハッシュ値を計算する
E24 署名を検証する
E25 関数値を計算する
E26 関数値を送付する
E27 関数値を受け取る

Fig.8