

【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 5 月 24 日 (2022.5.24)

【国際公開番号】 WO2021/053749
【出願番号】 特願 2021-546103 (P2021-546103)
【国際特許分類】
H 0 4 L 9/32 (2006.01)
G 0 6 F 21/32 (2013.01)
【F I】
H 0 4 L 9/32 2 0 0 C
G 0 6 F 21/32

10

【手続補正書】
【提出日】 令和 4 年 3 月 11 日 (2022.3.11)
【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】

20

登録のための第 1 入力データの第 1 コミットメントと、前記第 1 入力データが予め定められた入力データ空間に含まれていることを示す第 1 証明データとを生成する登録データ生成装置と、
前記第 1 コミットメントと前記第 1 証明データの一部又は全部を記憶する認証用データ記憶装置と、
前記第 1 コミットメントと前記第 1 証明データの検証を行う登録データ検証装置と、
前記第 1 コミットメントと前記第 1 証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、
認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと前記登録データ記憶装置の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを生成する認証データ生成装置と、
前記第 2 コミットメントと前記第 2 証明データの検証を行う認証データ検証装置とを備えた情報照合システム。

30

【請求項 2】
請求項 1 に記載の情報照合システムであって、
前記登録データ生成装置が生成する前記第 1 証明データの一部又は全部が、ゼロ知識証明によるデータである
ことを特徴とする情報照合システム。

40

【請求項 3】
請求項 1 又は 2 に記載の情報照合システムであって、
前記認証データ生成装置が生成する前記第 2 証明データの一部又は全部が、ゼロ知識証明によるデータである
ことを特徴とする情報照合システム。

【請求項 4】
請求項 1 ～ 3 のいずれか 1 項に記載の情報照合システムであって、
前記登録データ記憶装置に記憶された前記登録データが、前記第 1 入力データの前記第 1 コミットメントを含む

50

ことを特徴とする情報照合システム。

【請求項 5】

請求項 1～4 のいずれか 1 項に記載の情報照合システムであって、

前記認証用データ記憶装置に記憶された認証用データが、前記第 1 入力データの第 1 コミットメントを生成する際に用いた乱数を含む

ことを特徴とする情報照合システム。

【請求項 6】

請求項 1～5 のいずれか 1 項に記載の情報照合システムであって、

前記登録データ生成装置が生成する前記第 1 コミットメントの一部又は全部が、パラメータ g 、 h 、 N 、前記第 1 入力データ x 、乱数 r に対して、 $g^x \cdot h^r \bmod N$ である

ことを特徴とする情報照合システム。

【請求項 7】

請求項 1～6 のいずれか 1 項に記載の情報照合システムであって、

前記認証データ生成装置が生成する前記第 2 コミットメントの一部又は全部が、パラメータ g 、 h 、 N 、前記第 2 入力データ y 、乱数 r に対して、 $g^y \cdot h^r \bmod N$ である

ことを特徴とする情報照合システム。

【請求項 8】

登録のための第 1 入力データの第 1 コミットメントと、前記第 1 入力データが予め定められた入力データ空間に含まれていることを示す第 1 証明データとを含む登録データを生成する登録データ生成手段と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を記憶する認証用データ記憶手段と、

認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを生成する認証データ生成手段と

を備えたクライアント端末。

【請求項 9】

登録のための第 1 入力データの第 1 コミットメントと、前記第 1 入力データが予め定められた入力データ空間に含まれていることを示す第 1 証明データとを入力し、前記第 1 コミットメントと前記第 1 証明データの検証を行う登録データ検証手段と、

認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと登録データ記憶手段の登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを入力し、前記第 2 コミットメントと前記第 2 証明データの検証を行う認証データ検証手段と

の少なくとも一方を備えたサーバ。

【請求項 10】

登録のための第 1 入力データの第 1 コミットメントと、前記第 1 入力データが予め定められた入力データ空間に含まれていることを示す第 1 証明データとを生成する登録データ生成処理と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を記憶する認証用データ記憶処理と、

前記第 1 コミットメントと前記第 1 証明データの検証を行う登録データ検証処理と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、

認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを生成する認証データ生成処理と、

10

20

30

40

50

前記第 2 コミットメントと前記第 2 証明データの検証を行う認証データ検証処理とを含む情報照合方法。

【請求項 11】

登録のための第 1 入力データの第 1 コミットメントと、前記第 1 入力データが予め定められた入力データ空間に含まれていることを示す第 1 証明データとを生成する登録データ生成処理と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を記憶する認証用データ記憶処理と、

前記第 1 コミットメントと前記第 1 証明データの検証を行う登録データ検証処理と、

前記第 1 コミットメントと前記第 1 証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、

10

認証されるための第 2 入力データの第 2 コミットメントと、前記第 2 入力データが前記予め定められた入力データ空間に含まれていること及び前記第 2 入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第 2 証明データとを生成する認証データ生成処理と、

前記第 2 コミットメントと前記第 2 証明データの検証を行う認証データ検証処理とをコンピュータに実行させる情報照合プログラム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0009

20

【補正方法】変更

【補正の内容】

【0009】

例えば、生体から生成されていないデータを入力として、登録するためのデータを生成することや、認証を受けるためのデータを生成することも可能である。上述の加法準同型公開鍵暗号方式を利用した情報照合システム生体では、入力データを暗号化により秘匿していることから、上述の攻撃の例として、生体から生成されていないデータを用いて登録データを生成することにより、多くの生体特徴量と一致して認証受理と判定される登録データを生成すること、及び、認証時に利用された生体特徴量に関する情報を取得又は漏洩させるよう試みることなどの攻撃も想定される。また、生体から生成されていないデータを入力として認証を受けるデータを生成することにより、認証受理と判定され得るデータ（認証されるデータ）を生成することや、登録されている生体特徴量に関する情報を取得又は漏洩させるよう試みる攻撃も想定される。

30

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0080

【補正方法】変更

【補正の内容】

【0080】

(コミットメントフェーズ)

40

入力を v とし、 $Com(v, r) = g^v \cdot h^r \bmod N$ をコミットメントとする。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0099

【補正方法】変更

【補正の内容】

【0099】

ステップ A4 において識別子 (ID) を受信した登録データ生成装置 100 の認証用データ生成部 103 は、 $(ID, \{r_i\})$ を認証用データとして生成する (ステップ A8)。認証用データ生成部 103 は、認証用データを認証用データ記憶装置 400 に送付する

50

(ステップ A 9)。認証用データ記憶装置 4 0 0 は、認証用データを記憶する (ステップ A 1 0)。

10

20

30

40

50