【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６部門第２区分
【発行日】平成29年3月2日(2017.3.2)

【公開番号】特開2014-157354(P2014-157354A)
【公開日】平成26年8月28日(2014.8.28)
【年通号数】公開・登録公報2014-046
【出願番号】特願2014-26228(P2014-26228)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６４０Ｄ
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成29年1月26日(2017.1.26)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００６２
【補正方法】変更
【補正の内容】
【００６２】
本明細書および（適切な場合には）請求項および図面において開示される各特徴は、独立して、あるいは任意の適切な組み合わせにおいて与えられてもよい。ハードウェアで実装されるとして記述される特徴は、ソフトウェアで実装されてもよく、逆にソフトウェアで実装されるとして記述される特徴は、ハードウェアで実装されてもよい。請求項に参照符号があったとしても単に例示するものであって、請求項の範囲に対する限定効果はもたない。
いくつかの付記を記載しておく。
〔付記１〕
ベクトル
【数１２４】

$$(M_1, \ldots, M_n) \in \widehat{\mathbb{G}}^n$$

に対する線形準同型署名σを生成する方法であって、＾付きのGは第一の群を表わし、当該方法は、装置において：
・計算手段によって、署名鍵$sk=\{\chi_i, \gamma_i, \delta_i\}_{i=1}^{n}$を使って、
【数１２５】

$$z = \prod_{i=1}^{n} M_i^{-\chi_i},\ r = \prod_{i=1}^{n} M_i^{-\gamma_i},\ u = \prod_{i=1}^{n} M_i^{-\delta_i}$$

を計算することによって、署名要素(z,r,u)を計算する段階と；
・前記計算手段によって、前記署名要素(z,r,u)を含む署名σを出力する段階とを含む、方法。
〔付記２〕
前記署名鍵はさらに、要素

【数１２６】

$$h_z{}^{\alpha_r}$$

を含み、当該方法はさらに：
・前記計算手段によって、ランダムな要素
【数１２７】

$$\theta,\rho \overset{R}{\leftarrow} \mathbb{Z}_p$$

を選ぶ段階と；
・前記計算手段によって、さらなる署名要素v＝h$^{\rho}$を計算する段階とを含み、hは第二の群の要素であり；
zの前記計算はさらに、$g_r{}^{\theta}$による乗算を含み、rの前記計算はさらに$g_z{}^{-\theta}$による乗算を含み、uの前記計算はさらに
【数１２８】

$$(h_z{}^{\alpha_r})^{-\theta}$$

による乗算を含み、ここで、α_rは整数であり、h、g_rおよびg_zは前記第二の群の要素であり；
前記署名はさらに、前記署名要素vを含み；
前記第一の群および前記第二の群は同じである、
請求項１記載の方法。
〔付記３〕
ベクトル
【数１２９】

$$(M_1,\ldots,M_n) \in \hat{\mathbb{G}}^n$$

に対する署名要素(z,r,u)を含む線形準同型署名σを検証する方法であって、＾付きのGは第一の群を表わし、当該方法は、装置において：
・計算手段によって、
【数１３０】

$$(M_1,\ldots,M_n) \neq (1_{\hat{\mathbb{G}}},\ldots,1_{\hat{\mathbb{G}}})$$

であることおよび(z,r,u)が第一の等式
【数１３１】

$$1_{\mathbb{G}_T} = e(g_z,z)\cdot e(g_r,r)\cdot \prod_{i=1}^{n} e(g_i,M_i)$$

および第二の等式
【数１３２】

$$1_{\mathbb{G}_T} = e(h_z,z)\cdot\ e(h,u)\cdot \prod_{i=1}^{n} e(h_i,M_i)$$

を満たすことを検証する段階であって、e(・,・)は対称かつ可換なペアリングを表わし、h、h_z、h_i、g_r、g_iおよびg_zは第二の群の要素である、段階と；
・前記計算手段によって、前記検証が成功の場合に前記署名が成功裏に検証されたと判定

し、それ以外の場合に前記署名が成功裏に検証されなかったと判定する段階とを含む、方法。
〔付記４〕
前記第二の等式はさらに項
【数１３３】

$$e(H_{\mathbb{G}}(\tau), v)$$

を含み、ここで、$H_G(\tau)$はハッシュ関数を表わし、τは署名されたベクトルが存する部分空間の識別子を表わす、請求項３記載の方法。
〔付記５〕
ベクトル
【数１３４】

$$(M_1, \ldots, M_n) \in \hat{\mathbb{G}}^n$$

に対する線形準同型署名σを生成する装置であって、^付きのGは第一の群を表わし、当該装置はプロセッサを有し、該プロセッサは：
・署名鍵$sk=\{\chi_i, \gamma_i, \delta_i\}_{i=1}^{n}$を使って、
【数１３５】

$$z = \prod_{i=1}^{n} M_i^{-\chi_i},\ \ r = \prod_{i=1}^{n} M_i^{-\gamma_i},\ \ u = \prod_{i=1}^{n} M_i^{-\delta_i}$$

を計算することによって、署名要素(z,r,u)を計算する段階と；
・前記署名要素(z,r,u)を含む署名σを出力する段階とを実行するよう構成されている、装置。
〔付記６〕
前記署名鍵はさらに、要素
【数１３６】

$$h_z^{\alpha_r}$$

を含み、前記プロセッサはさらに：
・ランダムな要素
【数１３７】

$$\theta, \rho \xleftarrow{R} \mathbb{Z}_p$$

を選ぶ段階と；
・さらなる署名要素$v=h^{\rho}$を計算する段階とを実行するよう構成されており、ここで、hは第二の群の要素であり；
zの前記計算はさらに、g_r^{θ}による乗算を含み、rの前記計算はさらに$g_z^{-\theta}$による乗算を含み、uの前記計算はさらに
【数１３８】

$$(h_z^{\alpha_r})^{-\theta}$$

による乗算を含み、ここで、α_rは整数であり、h、g_rおよびg_zは前記第二の群の要素であり；
前記署名はさらに、前記署名要素vを含み；

前記第一の群および前記第二の群は同じである、
請求項５記載の装置。
〔付記７〕
ベクトル
【数１３９】

$$(M_1, \ldots, M_n) \in \hat{\mathbb{G}}^n$$

に対する署名要素(z,r,u)を含む線形準同型署名σを検証する装置であって、＾付きのGは第一の群を表わし、当該装置はプロセッサを有し、該プロセッサは：
・
【数１４０】

$$(M_1, \ldots, M_n) \neq (1_{\hat{\mathbb{G}}}, \ldots, 1_{\hat{\mathbb{G}}})$$

であることおよび(z,r,u)が第一の等式
【数１４１】

$$1_{\mathbb{G}_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i)$$

および第二の等式
【数１４２】

$$1_{\mathbb{G}_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^{n} e(h_i, M_i)$$

を満たすことを検証するよう構成されており、ここで、e(・,・)は対称かつ可換なペアリングを表わし、h、h_z、h_i、g_r、g_iおよびg_zは第二の群の要素であり；
前記プロセッサはさらに、前記検証が成功の場合に前記署名が成功裏に検証されたと判定し、それ以外の場合に前記署名が成功裏に検証されなかったと判定するよう構成されている、
装置。
〔付記８〕
前記第二の等式はさらに項
【数１４３】

$$e(H_{\mathbb{G}}(\tau), v)$$

を含み、ここで、H_G(τ)はハッシュ関数を表わし、τは署名されたベクトルが存する部分空間の識別子を表わす、請求項７記載の装置。
〔付記９〕
ベクトル
【数１４４】

$$(M_1, \ldots, M_n) \in \hat{\mathbb{G}}^n$$

に対する線形準同型署名σを生成する装置であって、＾付きのGは第一の群を表わし、当該装置はプロセッサを有し、該プロセッサは：
署名鍵

【数１４５】

$$\mathrm{sk} = \{h_z{}^{\alpha_r}, \chi_i, \gamma_i, \delta_i\}_{i=1}^{n}$$

を使って、
【数１４６】

$$z = g_r^{\theta} \cdot \prod_{i=1}^{n} M_i^{-\chi_i},\ r = g_z^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\gamma_i},\ u = (h_z{}^{\alpha_r})^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\delta_i},\ v = h^{\rho}$$

を計算することによって、署名要素(z,r,u,v)を計算するよう構成されており、
ここで、h_zは第二の群の元であり、α_rは整数であり、$H_G(\tau)$はハッシュ関数を表わし、τは署名されたベクトルが存する部分空間の識別子を表わし、
前記プロセッサはさらに：
z、rおよびuへのコミットメントをそれぞれ生成し；
z、rおよびuへの前記コミットメントを使って、z、rおよびuが所定の検証アルゴリズムを満たすことの証明を生成し；
署名要素vと、z、rおよびuへの前記コミットメントと、前記証明とを含む署名σを出力するよう構成されている、
装置。
〔付記１０〕
ベクトル
【数１４７】

$$(M_1, \dots, M_n) \in \widehat{\mathbb{G}}^n$$

に対する線形準同型署名σを検証する装置であって、＾付きのGは第一の群を表わし、前記線形準同型署名σは第一の署名要素v、それぞれさらなる署名要素z、rおよびuへのコミットメント
【数１４８】

$$\vec{C}_z, \vec{C}_r, \vec{C}_u$$

およびz、rおよびuが所定の検証アルゴリズムを満たすことの証明
【数１４９】

$$\vec{\pi}_1, \vec{\pi}_2$$

を含み、前記コミットメントはベクトル
【数１５０】

$$\vec{f}_1, \vec{f}_2, \vec{f}_3$$

を使って生成されたものであり、当該装置はプロセッサを有し、該プロセッサは、
【数１５１】

$$(M_1, \dots, M_n) \neq (1_{\widehat{\mathbb{G}}}, \dots, 1_{\widehat{\mathbb{G}}})$$

であることおよび検証

【数１５２】

$$\prod_{i=1}^{n} E\left(g_i,(1_{\mathbb{G}},1_{\mathbb{G}},M_i)\right)^{-1}=E\left(g_z,\vec{C}_z\right)\cdot E\left(g_r,\vec{C}_r\right)\cdot E\left(\pi_{1,1},\vec{f}_1\right)\cdot E\left(\pi_{1,2},\vec{f}_2\right)\cdot E\left(\pi_{1,3},\vec{f}_3\right)$$

かつ

$$\prod_{i=1}^{n} E\left(h_i,(1_{\mathbb{G}},1_{\mathbb{G}},M_i)\right)^{-1}\cdot E\left(H_{\mathbb{G}}(\tau),(1_{\mathbb{G}},1_{\mathbb{G}},v)\right)^{-1}=E\left(h_z,\vec{C}_z\right)\cdot E\left(h,\vec{C}_u\right)\cdot E\left(\pi_{2,1},\vec{f}_1\right)\cdot E\left(\pi_{2,2},\vec{f}_2\right)\cdot E\left(\pi_{2,3},\vec{f}_3\right),$$

を検証するよう構成されており、

ここで、E(・,・)は座標ごとのペアリングを表わし、h、h_z、h_j、g_r、g_jおよびg_zは第二の群の要素であり；

前記プロセッサはさらに：

前記検証が成功の場合に前記署名が成功裏に検証されたと判定し、それ以外の場合に前記署名が成功裏に検証されなかったと判定するよう構成されている、

装置。