

【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】令和 3 年 9 月 9 日 (2021.9.9)

【公開番号】特開 2020-56960 (P2020-56960A)

【公開日】令和 2 年 4 月 9 日 (2020.4.9)

【年通号数】公開・登録公報 2020-014

【出願番号】特願 2018-188781 (P2018-188781)

【国際特許分類】

G 0 9 C 1/00 (2006.01)

【F I】

G 0 9 C 1/00 6 2 0 Z

【手続補正書】

【提出日】令和 3 年 8 月 2 日 (2021.8.2)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】0 0 0 7

【補正方法】変更

【補正の内容】

【0 0 0 7】

【図 1】実施の形態 1 に係る暗号システム 1 の構成図。

【図 2】実施の形態 1 に係るセットアップ装置 10 の構成図。

【図 3】実施の形態 1 に係る暗号化装置 20 の構成図。

【図 4】実施の形態 1 に係る鍵生成装置 30 の構成図。

【図 5】実施の形態 1 に係る復号装置 40 の構成図。

【図 6】実施の形態 1 に係るセットアップ装置 10 の動作を示すフローチャート。

【図 7】実施の形態 1 に係る暗号化装置 20 の動作を示すフローチャート。

【図 8】実施の形態 1 に係る鍵生成装置 30 の動作を示すフローチャート。

【図 9】実施の形態 1 に係る P G B 計算処理を示すフローチャート。

【図 10】実施の形態 1 に係る復号装置 40 の動作を示すフローチャート。

【図 11】実施の形態 1 に係る復号処理を示すフローチャート。

【図 12】変形例 3 に係るセットアップ装置 10 の構成図。

【図 13】変形例 3 に係る暗号化装置 20 の構成図。

【図 14】変形例 3 に係る鍵生成装置 30 の構成図。

【図 15】変形例 3 に係る復号装置 40 の構成図。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0 0 4 7

【補正方法】変更

【補正の内容】

【0 0 4 7】

図 2 を参照して、実施の形態 1 に係るセットアップ装置 10 の構成を説明する。

セットアップ装置 10 は、P H P E . S e t u p アルゴリズムを実行するコンピュータである。

セットアップ装置 10 は、プロセッサ 11 と、メモリ 12 と、ストレージ 13 と、通信インタフェース 14 とのハードウェアを備える。プロセッサ 11 は、信号線を介して他のハードウェアと接続され、これら他のハードウェアを制御する。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】 0 0 7 9

【補正方法】 変更

【補正の内容】

【0 0 7 9】

(ステップ S 3 3 2 : 関数 ρ 生成処理)

PGB 計算部 3 1 3 は、 $j' \in [m]$ の各整数 j' について、行列表現 L の j' 行に変数 $x_{j'}$ が含まれるなら、 $\rho(j') = i'$ と設定することにより、関数 $\rho : [m] \rightarrow [n']$ を生成する。PGB 計算部 3 1 3 は、関数 ρ をメモリ 3 2 に書き込む。

【手続補正 4】

【補正対象書類名】 明細書

【補正対象項目名】 0 0 8 0

【補正方法】 変更

【補正の内容】

【0 0 8 0】

(ステップ S 3 3 3 : 定数計算処理)

PGB 計算部 3 1 3 は、数 1 4 9 に示すように、ベクトル $r \rightarrow$ を選択する。

【数 1 4 9】

$$\vec{r} \leftarrow \frac{U}{q} \mathbb{F}_q^{m+n-1}$$

PGB 計算部 3 1 3 は、ステップ S 3 3 1 で生成された行列表現 L と、ベクトル $r \rightarrow$ とを用いて、数 1 5 0 に示すように、定数の集合 $(\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]}) \in \mathbb{F}_q^n \times (\mathbb{F}_q^2)^m$ を計算する。

【数 1 5 0】

$$L \begin{pmatrix} \vec{r}^T \\ 1 \end{pmatrix} = (\alpha_1 x_{\rho(1)} + \gamma_1, \dots, \alpha_m x_{\rho(m)} + \gamma_m, z_1 + \sigma_1, \dots, z_n + \sigma_n)^T$$

これにより、定数の集合 $(\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]})$ が生成される。PGB 計算部 3 1 3 は、定数の集合 $(\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]})$ をメモリ 3 2 に書き込む。この定数の集合 $(\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]})$ を ABP の述語ベクトルと呼ぶ。

【手続補正 5】

【補正対象書類名】 明細書

【補正対象項目名】 0 1 3 8

【補正方法】 変更

【補正の内容】

【0 1 3 8】

1 暗号システム、1 0 セットアップ装置、1 1 プロセッサ、1 2 メモリ、1 3 ストレージ、1 4 通信インタフェース、1 5 電子回路、1 1 1 受付部、1 1 2 マスター鍵生成部、1 1 3 送信部、2 0 暗号化装置、2 1 プロセッサ、2 2 メモリ、2 3 ストレージ、2 4 通信インタフェース、2 5 電子回路、2 1 1 マスター鍵取得部、2 1 2 ベクトル取得部、2 1 3 暗号化部、2 1 4 送信部、3 0 鍵生成装置、3 1 プロセッサ、3 2 メモリ、3 3 ストレージ、3 4 通信インタフェース、3 5 電子回路、3 1 1 マスター鍵取得部、3 1 2 関数取得部、3 1 3 PGB 計算部、3 1 4 鍵生成部、3 1 5 送信部、4 0 復号装置、4 1 プロセッサ、4 2 メモリ、4 3 ストレージ、4 4 通信インタフェース、4 5 電子回路、4 1 1 マス

ター鍵取得部、412 暗号文取得部、413 復号鍵取得部、414 復号部、415 余因子計算部、416 ペアリング演算部、417 出力値計算部。

【手続補正6】

【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】

双対ベクトル空間における双対基底である基底 B 及び基底 B^* のうちの基底 B に、属性ベクトルと、 ABP (Arithmetic Branching Programs) の述語ベクトルとの一方が設定された暗号文を取得する暗号文取得部と、

前記基底 B^* に、前記属性ベクトルと前記述語ベクトルとの他方が設定された復号鍵を取得する復号鍵取得部と、

前記暗号文取得部によって取得された前記暗号文と、前記復号鍵取得部によって取得された前記復号鍵とについてペアリング演算を行うことにより、前記暗号文を復号する復号部と

を備える復号装置。

【請求項2】

前記述語ベクトルの要素は、関数 f を計算する ABP を表す行列表現 L と、最後の行の要素が1である行列との積によって得られた要素である

請求項1に記載の復号装置。

【請求項3】

前記復号部は、

前記行列表現 L の最後の列の要素の余因子を計算する余因子計算部と、

前記暗号文と前記復号鍵とについてペアリング演算を行うことにより演算値を計算するペアリング演算部と、

前記余因子計算部によって計算された前記余因子と、前記ペアリング演算部によって計算された前記演算値とから、前記暗号文を復号して得られる出力値を計算する出力値計算部と

を備える請求項2に記載の復号装置。

【請求項4】

前記出力値計算部は、内積と前記余因子とから、前記関数 f に前記属性ベクトルを入力した値を計算して、計算された値により前記出力値を計算する

請求項3に記載の復号装置。

【請求項5】

前記暗号文取得部は、数1に示す暗号文 CT を取得し、

前記復号鍵取得部は、数2に示す復号鍵 $SK(f)$ を取得し、

前記ペアリング演算部は、数3に示すようにペアリング演算を行うことにより、前記演算値 Λ'_j , Λ_j を計算し、

前記出力値計算部は、数4に示すように値 Λ を計算して、前記値 Λ の値に応じて出力値を計算する

請求項4に記載の復号装置。

【数 1】

$$CT = (\vec{x}, \{c^{(l')}\}_{l' \in [n']}, \{c^{(l)}\}_{l \in [n]})$$

$$\omega \xleftarrow{U} \mathbb{F}_q,$$

for $l' \in [n']$

$$\phi_{l'} \xleftarrow{U} \mathbb{F}_q, c^{(l')} = (\omega(1, x_{l'}), \vec{0}^4, \vec{0}^2, \phi_{l'})_{\mathbb{B}_{l'}},$$

for $l \in [n]$

$$\phi_l \xleftarrow{U} \mathbb{F}_q, c^{(l)} = (\omega(1, z_l), \vec{0}^4, \vec{0}^2, \phi_l)_{\mathbb{B}_{n'+l}},$$

 $n', n \in \mathbb{N},$ $(\vec{x}, \vec{z}) \in \mathbb{F}_q^{n'} \times \mathbb{F}_q^n$ は属性ベクトル

【数 2】

$$SK(f) = (f, \{k^{(j')}\}_{j' \in [m]}, \{k^{(j)}\}_{j \in [n]}),$$

$$((\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]}), \rho : [m] \rightarrow [n']) \xleftarrow{R} PGB(f),$$

$$\varsigma \xleftarrow{U} \mathbb{F}_q,$$

for $j' \in [m]$

$$\vec{k}^{(j')} \xleftarrow{U} \mathbb{F}_q^2, k^{(j')} = ((\gamma_{j'}, \alpha_{j'}), \vec{0}^4, \vec{k}^{(j')}, 0)_{\mathbb{B}_{\rho(j')}^*},$$

for $j \in [n]$

$$\vec{k}^{(j)} \xleftarrow{U} \mathbb{F}_q^2, k^{(j)} = ((\sigma_j, \varsigma), \vec{0}^4, \vec{k}^{(j)}, 0)_{\mathbb{B}_{n'+j}^*},$$

 $PGB(f)$ は、関数 f を入力として、関数 $\rho : [m] \rightarrow [n']$ を伴う述語ベクトルの要素である定数の集合 $(\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]}) \in \mathbb{F}_q^n \times (\mathbb{F}_q^2)^m$ を出力するアルゴリズム,

【数 3】

$$\Lambda_{j'} = e(c^{(\rho(j'))}, k^{(j')}) \text{ for } j' \in [m],$$

$$\Lambda_j = e(c^{(j)}, k^{(j)}) \text{ for } j \in [n]$$

【数 4】

$$\Lambda = \left(\prod_{j' \in [m]} \Lambda'_{j'} \Omega'_{j'} \right) \left(\prod_{j \in [n]} \Lambda_j \Omega_j \right),$$

$$(\{\Omega_j\}_{j \in [n]}, \{\Omega'_{j'}\}_{j' \in [m]}) = REC(f, \vec{x}),$$

$REC(f, \vec{x})$ は、関数 f と、 $\vec{x} \in F_q^{n'}$ とを入力として、係数の集合 $(\{\Omega_j\}_{j \in [n]},$

$\{\Omega'_{j'}\}_{j' \in [m]}) \in F_q^{n+m}$ を出力するアルゴリズム

【請求項 6】

前記暗号文取得部は、数 5 に示す暗号文 CT を取得し、

前記復号鍵取得部は、数 6 に示す復号鍵 $SK(f)$ を取得し、

前記ペアリング演算部は、数 7 に示すようにペアリング演算を行うことにより、前記演算値 $\Lambda'_0, \Lambda'_j, \Lambda_j$ を計算し、

前記出力値計算部は、数 8 に示すように値 Λ を計算して、前記値 $\Lambda \Lambda'_0$ を前記出力値として計算する

請求項 4 に記載の復号装置。

【数 5】

$$CT = (\vec{x}, \{c^{(\iota')}\}_{\iota' \in [0, n']}, \{c^{(\iota)}\}_{\iota \in [n]}),$$

$$\omega, \xi, \phi'_0 \xleftarrow{U} \mathbb{F}_q,$$

$$c^{(0)} = (\omega, \vec{0}^2, \xi, 0, \phi'_0)_{\mathbb{B}_0},$$

for $\iota' \in [n']$

$$\phi'_{\iota'} \xleftarrow{U} \mathbb{F}_q, c^{(\iota')} = (\omega(1, x_{\iota'}), \vec{0}^4, \vec{0}^2, \phi'_{\iota'})_{\mathbb{B}_{\iota'}},$$

for $\iota \in [n]$

$$\phi_{\iota} \xleftarrow{U} \mathbb{F}_q, c^{(\iota)} = (\omega(1, z_{\iota}), \vec{0}^4, \vec{0}^2, \phi_{\iota})_{\mathbb{B}_{n'+\iota}},$$

$n', n \in \mathbb{N},$

$(\vec{x}, \vec{z}) \in \mathbb{F}_q^{n'} \times \mathbb{F}_q^n$ は属性ベクトル

【数 6】

$$SK(f) = (f, \{\beta'_{j'}\}_{j' \in [m]}, \{\beta_j\}_{j \in [n]}, \{k'(j')\}_{j' \in [0, m]}, \{k(j)\}_{j \in [n]}),$$

$$((\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]}), \rho: [m] \rightarrow [n']) \xleftarrow{R} PGB(f),$$

$$r_0, \kappa'_0, \varsigma \xleftarrow{U} \mathbb{F}_q,$$

$$k'(0) = (-r_0, \vec{0}^2, 1, \kappa'_0, 0)_{\mathbb{B}_0^*},$$

for $j' \in [m]$

$$\beta'_{j'} \xleftarrow{U} \mathbb{F}_q, \quad \vec{\kappa}'(j') \xleftarrow{U} \mathbb{F}_q^2,$$

$$\gamma_{j'}^+ = \gamma_{j'} + \beta'_{j'} r_0, \quad k'(j') = ((\gamma_{j'}^+, \alpha_{j'}), \vec{0}^4, \vec{\kappa}'(j'), 0)_{\mathbb{B}_{\rho(j')}^*},$$

for $j \in [n]$

$$\beta_j \xleftarrow{U} \mathbb{F}_q, \quad \vec{\kappa}(j) \xleftarrow{U} \mathbb{F}_q^2,$$

$$\sigma_j^+ = \sigma_j + \beta_j r_0, \quad k(j) = ((\sigma_j^+, \varsigma), \vec{0}^4, \vec{\kappa}(j), 0)_{\mathbb{B}_{n'+j}^*},$$

$PGB(f)$ は、関数 f を入力として、関数 $\rho: [m] \rightarrow [n']$ を伴う述語ベクトルの要素である定数の集合 $(\{\sigma_j\}_{j \in [n]}, \{\alpha_{j'}, \gamma_{j'}\}_{j' \in [m]}) \in \mathbb{F}_q^n \times (\mathbb{F}_q^2)^m$ を出力するアルゴリズム,

【数 7】

$$\Lambda'_0 = e(c'(0), k'(0)),$$

$$\Lambda'_{j'} = e(c'(\rho(j')), k'(j')) \text{ for } j' \in [m],$$

$$\Lambda_j = e(c(j), k(j)) \text{ for } j \in [n]$$

【数 8】

$$\Lambda = \left(\prod_{j' \in [m]} \Lambda'_{j'} \Omega'_{j'} \right) \left(\prod_{j \in [n]} \Lambda_j \Omega_j \right)^{\frac{1}{\sum_{j' \in [m]} \Omega'_{j'} \beta'_{j'} + \sum_{j \in [n]} \Omega_j \beta_j}},$$

$$(\{\Omega_j\}_{j \in [n]}, \{\Omega'_{j'}\}_{j' \in [m]}) = REC(f, \vec{x}),$$

$REC(f, \vec{x})$ は、関数 f と、 $\vec{x} \in F_q^{n'}$ とを入力として、係数の集合 $(\{\Omega_j\}_{j \in [n]},$

$\{\Omega'_{j'}\}_{j' \in [m]}) \in F_q^{n+m'}$ を出力するアルゴリズム

【請求項 7】

双対ベクトル空間における双対基底である基底 B 及び基底 B^* のうちの基底 B に、属性ベクトルと、 ABP (Arithmetic Branching Programs) の述語ベクトルとの一方を設定して暗号文を生成する暗号化装置と、

前記基底 B^* に、前記属性ベクトルと前記述語ベクトルとの他方を設定して復号鍵を生成する鍵生成装置と、

前記暗号化装置によって生成された前記暗号文と、前記鍵生成装置によって生成された前記復号鍵とについてペアリング演算を行うことにより、前記暗号文を復号する復号装置と

を備える暗号システム。

【請求項 8】

暗号文取得部が、双対ベクトル空間における双対基底である基底 B 及び基底 B^* のうちの基底 B に、属性ベクトルと、 ABP (Arithmetic Branching Programs) の述語ベクトルとの一方が設定された暗号文を取得し、

復号鍵取得部が、前記基底 B^* に、前記属性ベクトルと前記述語ベクトルとの他方が設定された復号鍵を取得し、

復号部が、前記暗号文取得部によって取得された前記暗号文と、前記復号鍵取得部によって取得された前記復号鍵とについてペアリング演算を行うことにより、前記暗号文を復号する復号方法。

【請求項 9】

暗号文取得部が、双対ベクトル空間における双対基底である基底 B 及び基底 B^* のうちの基底 B に、属性ベクトルと、 ABP (Arithmetic Branching Programs) の述語ベクトルとの一方が設定された暗号文を取得する暗号文取得処理と、

復号鍵取得部が、前記基底 B^* に、前記属性ベクトルと前記述語ベクトルとの他方が設定された復号鍵を取得する復号鍵取得処理と、

復号部が、前記暗号文取得処理によって取得された前記暗号文と、前記復号鍵取得処理によって取得された前記復号鍵とについてペアリング演算を行うことにより、前記暗号文を復号する復号処理と

を行う復号装置としてコンピュータを機能させる復号プログラム。