

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年9月24日(24.09.2020)



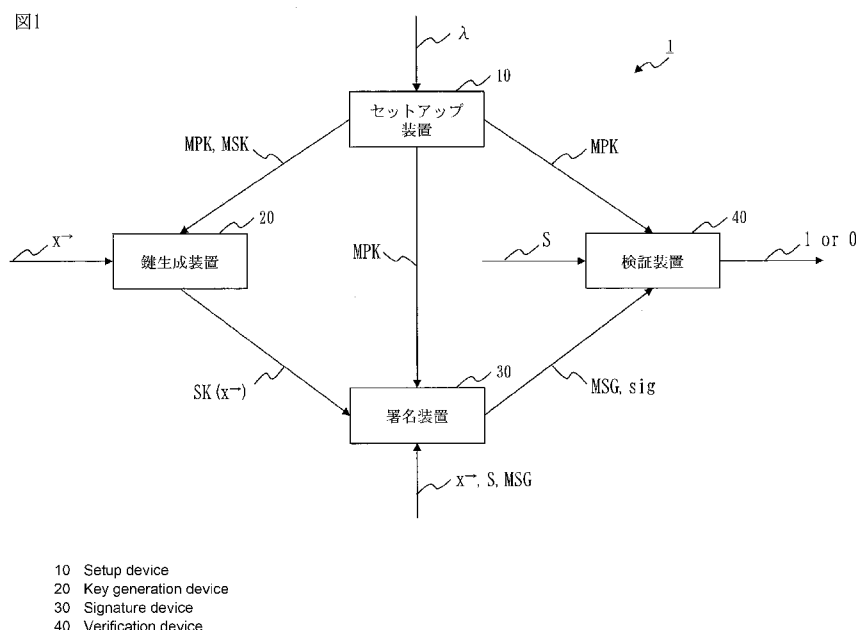
(10) 国際公開番号

WO 2020/188906 A1

- (51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/32* (2006.01)
H04L 9/14 (2006.01)
- (21) 国際出願番号: PCT/JP2019/047995
- (22) 国際出願日: 2019年12月9日(09.12.2019)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2019-048622 2019年3月15日(15.03.2019) JP
- (71) 出願人: 三菱電機株式会社(MITSUBISHI ELECTRIC CORPORATION) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP). 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).
- (72) 発明者: 高島 克幸(TAKASHIMA, Katsuyuki); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 岡本 龍明(OKAMOTO, Tatsuaki); 〒1808585 東京都武蔵野市緑町三丁目9番11号 N T T 知的財産センタ内 Tokyo (JP). ダッタ プラティッシュ(DATTA, Pratish); 〒1808585 東京都武蔵野市緑町三丁目9番11号 N T T 知的財産センタ内 Tokyo (JP).
- (74) 代理人: 溝井 国際特許業務法人(MIZOI INTERNATIONAL PATENT FIRM);

(54) Title: SIGNATURE DEVICE, VERIFICATION DEVICE, SIGNATURE METHOD, VERIFICATION METHOD, SIGNATURE PROGRAM, AND VERIFICATION PROGRAM

(54) 発明の名称: 署名装置、検証装置、署名方法、検証方法、署名プログラム及び検証プログラム



(57) Abstract: A signature device (30) acquires a signature key SK ($x^{\rightarrow}$) in which an attribute vector $x^{\rightarrow}$ is set to a basis B^* of a basis B and the basis B^* , which are a dual basis in a dual vector space. The signature device (30) sets predicate information of arithmetic branching programs (ABP) to the signature key SK ($x^{\rightarrow}$) and generates a signature sig with respect to a message MSG. The signature device (30) outputs the signature sig and the message

〒2470056 神奈川県鎌倉市大船二丁目 1 7
番 1 0 号 3 階 Kanagawa (JP).

- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告 (条約第21条(3))

MSG to a verification device (40).

(57) 要約: 署名装置 (30) は、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 x^* が設定された署名鍵 $SK(x^*)$ を取得する。署名装置 (30) は、署名鍵 $SK(x^*)$ に対して、ABP (Arithmetic Branching Programs) の述語情報を設定して、メッセージ MSG に対する署名 sig を生成する。署名装置 (30) は、署名 sig と、メッセージ MSG とを検証装置 (40) に出力する。

明 細 書

発明の名称：

署名装置、検証装置、署名方法、検証方法、署名プログラム及び検証プログラム

技術分野

[0001] この発明は、ABP (A r i t h m e t i c B r a n c h i n g P r o g r a m s) を用いた署名技術に関する。

背景技術

[0002] 非特許文献1には、多項式サイズ回路及び多項式時間計算可能チューリングマシン等により決まる一般的な述語に対する属性ベース署名 (ABS : A t t r i b u t e - B a s e d S i g n a t u r e) 方式が記載されている。

先行技術文献

非特許文献

[0003] 非特許文献1 : Y. S a k a i , S. K a t s u m a t a , N. A t t r a p a d u n g , G. H a n a o k a , A t t r i b u t e - b a s e d s i g n a t u r e s f o r u n b o u n d e d l a n g u a g e s f r o m s t a n d a r d a s s u m p t i o n s

発明の概要

発明が解決しようとする課題

[0004] しかし、非特許文献1に記載された方式は、極めて理論的で実際に使える効率性を達成することは困難であった。

この発明は、実用的なABE方式を構成可能にすることを目的とする。

課題を解決するための手段

[0005] この発明に係る署名装置は、
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、属性ベクトルが設定された署名鍵を取得する取得部と、

前記取得部によって取得された前記署名鍵に対して、ABP (Arithmetic Branching Programs) の述語情報を設定して、メッセージに対する署名を生成する署名部と、

前記署名部によって生成された前記署名と、前記メッセージとを出力する出力部と

を備える。

発明の効果

[0006] この発明では、属性ベクトルが設定された署名鍵に対して、ABPの述語ベクトルを設定して署名を生成する。これにより、実用的なABE方式を構成することが可能になる。

図面の簡単な説明

[0007] [図1]実施の形態1に係る署名システム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に係る鍵生成装置20の構成図。

[図4]実施の形態1に係る署名装置30の構成図。

[図5]実施の形態1に係る検証装置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に係る鍵生成装置20の動作を示すフローチャート。

[図8]実施の形態1に係る署名装置30の動作を示すフローチャート。

[図9]実施の形態1に係る検証装置40の動作を示すフローチャート。

[図10]変形例2に係るセットアップ装置10の構成図。

[図11]変形例2に係る鍵生成装置20の構成図。

[図12]変形例2に係る署名装置30の構成図。

[図13]変形例2に係る検証装置40の構成図。

発明を実施するための形態

[0008] 実施の形態1.

表記

以下の説明で用いる表記を説明する。

数 1 0 1 は、セキュリティパラメータを示し、 1^λ は、単進符号のエンコーディングを表す。

[数101]

$$\lambda \in \mathbb{N}$$

[0009] 数 1 0 2 は、 q を法とする有限体を示す。数 1 0 2 は、体 F_q 又は単に F_q と記載される。

[数102]

$$\mathbb{F}_q \text{ for any prime } q \in \mathbb{N}$$

[0010] 数 1 0 3 に対して、数 1 0 4 とする。

[数103]

$$\begin{aligned} d &\in \mathbb{N}, \\ c &\in \mathbb{N} \cup \{0\} \ (c < d) \end{aligned}$$

[数104]

$$\begin{aligned} [d] &= \{1, \dots, d\}, \\ [c, d] &= \{c, \dots, d\} \end{aligned}$$

[0011] 数 1 0 5 は、集合 Z から要素 z を一様にサンプリングする処理を示す。

[数105]

$$z \xleftarrow{U} Z$$

Z は、集合 Z のサイズ又は濃度を示す。

[0012] 確率的アルゴリズム P に対して、数 1 0 6 は、一様なランダムテープを伴う入力 Θ におけるアルゴリズム P の出力分布から Π をサンプリング処理を示す。

[数106]

$$\Pi \xleftarrow{R} P(\Theta)$$

確定的アルゴリズムDに対して、 $\Pi = D(\Theta)$ は、入力 Θ におけるアルゴリズムDの出力を示す。

[0013] アルゴリズムは、内容から明らかな場合には、入力として明示されていない場合であっても、セキュリティパラメータ λ の単進符号表現 1^λ が入力として与えられるものとする。

[0014] 数107に対して、数108は、数109に示すベクトルを示す。また、数108は、 $\vec{v}$ と記載される。

[数107]

$$\mathbb{F}_q, d \in \mathbb{N}$$

[数108]

$$\vec{v}$$

[数109]

$$(v_1, \dots, v_d) \in \mathbb{F}_q^d$$

$$\text{where } v_i \in \mathbb{F}_q \text{ for all } i \in [d]$$

[0015] 体 $\mathbb{F}_q^d$ における全てが0のベクトルは、数110のように記載される。

[数110]

$$\vec{0}^d$$

また、体 $\mathbb{F}_q^d$ における正規基底ベクトルは、数111のように表される。

[数111]

$$\vec{e}^{(d,i)} = (\overbrace{0, \dots, 0}^{i-1}, \overbrace{1, 0, \dots, 0}^{d-i}) \text{ for } i \in [d]$$

[0016] 数112に示す2つのベクトルに対して、数113は、ベクトル $\vec{v}$ とベクトル

ル $w \rightarrow$ との内積を示す。つまり、数 1 1 3 は、数 1 1 4 を示す。

[数112]

$$\vec{v}, \vec{w} \in \mathbb{F}_q^d$$

[数113]

$$\vec{v} \cdot \vec{w}$$

[数114]

$$\vec{v} \cdot \vec{w} = \sum_{i \in [d]} v_i w_i \in \mathbb{F}_q$$

[0017] 数 1 1 5 は、数 1 1 6 によって張られた体 $\mathbb{F}_q^d$ の部分空間を示す。

[数115]

$$\text{for any } s \in \mathbb{N}, \text{ and any } \{\vec{v}^{(i)}\}_{i \in [s]} \subset \mathbb{F}_q^d$$

$$\text{SPAN} \langle \vec{v}^{(i)} \mid i \in [s] \rangle$$

[数116]

$$\{\vec{v}^{(i)}\}_{i \in [s]}$$

[0018] 数 1 1 7 は、乗法巡回群を示す。数 1 1 7 は、群 G 又は単に G と記載される。

[数117]

$$G$$

群 G と、群 G の生成元 g とに対して、 v は群要素の d 次元ベクトルを示す。つまり、数 1 1 8 である。

[数118]

$$v = (g^{v_1}, \dots, g^{v_d}) \in \mathbb{G}^d \text{ for some } d \in \mathbb{N},$$

$$\text{where } \vec{v} = (v_1, \dots, v_d) \in \mathbb{F}_q^d$$

[0019] $M = (m_{k,i})$ は、成分 $m_{k,i} \in \mathbb{F}_q$ を有する $d \times r$ 行列を示す。 M^T は、行列 M の転置行列を示す。 $\det(M)$ は、行列 M の行列式を示す。行列の記載において、 I は、単位行列を示し、 O は、ゼロ行列を示す。 $GL(d, \mathbb{F}_q)$ は、 $\mathbb{F}_q^{d \times d}$ における全ての $d \times d$ の可逆行列の集合を示す。

[0020] ***準備***

以下の説明で用いられる用語の定義等を説明する。

[0021] 実施の形態1では、ABPの述語を用いたABS方式を説明する。また、実施の形態1では、ABPの述語のASP (Arithmetic Span Programs) 表現を用いる。そこで、ABP及びASPについて説明する。

[0022] <ABP>

BP (Branching Program) Γ は、数119に示す5つの要素によって定義される。

[数119]

$$\Gamma = (V, E, V_0, V_1, \phi)$$

数120は頂点の集合を示し、数121は辺の集合を示す。数120は、単に V と記載され、数121は、単に E と記載される。

[数120]

$$V$$

[数121]

$$E$$

(V, E) は、有効非巡回グラフである。 $V_0, V_1 \in V$ は、それぞれソー

スとシンクと呼ばれる特別な頂点である。 ϕ は、 E における辺に対するラベリング関数である。

[0023] 有限体 F_q における $ABP\Gamma$ は、数122に示す関数 f を計算する。

[数122]

$$f: F_q^n \rightarrow F_q \text{ for some } n \in N$$

ここで、 E における各辺に割り当てられるラベリング関数 ϕ は、 F_q における係数を伴う1つの変数の1次式、又は、 F_q における定数である。 p を、 $ABP\Gamma$ におけるソース V_0 からシンク V_1 への全てのパスの集合とする。ある入力 $x \mapsto (x_1, \dots, x_d) \in F_q^d$ における $ABP\Gamma$ によって計算される関数 f の出力は、数123に示すように定義される。

[数123]

$$f(\vec{x}) = \sum_{P \in \mathcal{P}} \left[\prod_{E \in P} \phi(E) |_{\vec{x}} \right]$$

数124は、 $x \mapsto$ に対する関数 $\phi(E)$ の評価値を示す。

[数124]

$$E \in \mathcal{E}, \phi(E) |_{\vec{x}}$$

[0024] 非特許文献Ishai, Y., Kushilevitz, E.: Perfect constant-round secure computation via perfect randomizing polynomials. In: International Colloquium on Automata, Languages, and Programming-ICALP 2002. pp. 244-256. Springer (2002) には、次の内容が示されている。

関数 f を計算する $ABP\Gamma = (V, E, V_0, V_1, \phi)$ が与えられた場合、入力 $x \mapsto \in F_q^d$ を F_q における $(\#V - 1) \times (\#V - 1)$ の行列 $L(x \mapsto)$

にマッピングする関数 L を効率的かつ決定的に計算することが可能である。

また、以下の (1) から (3) が成立する。

(1) $\det(L(x^-)) = f(x^-)$ である。

(2) $(L(x^-))$ の各成分は、 F_q における係数を伴う 1 つの変数 x_i ($i \in [d]$) の 1 次式、又は、 F_q における定数である。

(3) $(L(x^-))$ は、第 2 対角、つまり主対角のすぐ下の対角には、 -1 だけを含み、第 2 対角の下には 0 だけを含む。

具体的には、行列 L は、行列 $A_{\Gamma-1}$ から、 V_0 に対応する列と、 V_1 に対応する行と

を取り除くことによって得られる。ここで、行列 A_{Γ} は、 Γ に対する隣接行列である。 I は単位行列である。

[0025] ここで、ブーリアン方式と、ブーリアンブランチングプログラムと、算術方式とを ABP に変換する線形時間アルゴリズムが存在する。

[0026] $\langle ASP \rangle$

n 個の変数におけるアクセスストラクチャ $S = (U, \rho)$ は、数 1 2 5 に示すベクトルのペアの集合 U と、数 1 2 6 に示す関数 ρ とである。

[数125]

$$U = \{\vec{y}^{(j)}, \vec{z}^{(j)}\}_{j \in [m]} \text{ for } m \in \mathbb{N},$$

$$\text{where for all } j \in [m], (\vec{y}^{(j)}, \vec{z}^{(j)}) \in (\mathbb{F}_q^L)^2 \text{ for } L \in \mathbb{N}$$

[数126]

$$\rho: [m] \rightarrow [n]$$

数 1 2 7 である場合に限り、数 1 2 8 に示す属性ベクトル x^- はアクセスストラクチャ S を満たす。

[数127]

$$\vec{e}^{(L,L)} \in \text{SPAN} \left\langle x_{\rho(j)} \vec{y}^{(j)} + \vec{z}^{(j)} \mid j \in [m] \right\rangle$$

[数128]

$$\vec{x} \in \mathbb{F}_q^n$$

[0027] ABPとASPとは、以下のように関連付けられる。

数129に対して、数130に示す関数 f を計算するサイズ $m+1$ の ABP $\Gamma = (V, E, V_0, V_1, \phi)$ が与えられた場合に、数131に示す ASP のアクセスストラクチャ S を構築する効率的なアルゴリズムがあることが、非特許文献 Ishai, Y., Wee, H.: Partial garbling schemes and their applications. In: ICALP 2014. pp. 650-662. Springer に示されている。

[数129]

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

[数130]

$$f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q$$

[数131]

$$\mathcal{S} = (\mathcal{U} = \{\vec{y}^{(j)}, \vec{z}^{(j)}\}_{j \in [m]} \subset (\mathbb{F}_q^{(m+1)})^2, \rho: [m] \rightarrow [n])$$

such that for all $\vec{x} \in \mathbb{F}_q^n$, $f(\vec{x}) = 0 \Leftrightarrow \mathcal{S}$ accepts $\vec{x}$

ここで、数132は、 $f(\vec{x}) = 0$ と、アクセスストラクチャ S が $\vec{x}$ を受理することとが同値であることを意味する。

[数132]

$$f(\vec{x}) = 0 \Leftrightarrow \mathcal{S} \text{ accepts } \vec{x}$$

[0028] 実施の形態1では、双対ベクトル空間である双対ペアリングベクトル空間 (DPVS: Dual Pairing Vector Spaces) に

において、ABSを実現する。そこで、DPVSと、DPVSの前提となる双線形群とについて説明する。

[0029] <双線形群>

数133に示す双線形群である params_G は、素数 q と、位数 q の乗法巡回群 G_1 、 G_2 、 G_T と、群 G_1 の生成元 g_1 と、群 G_2 の生成元 g_2 と、数134に示す双線形写像 e とを備える。

[数133]

$$\text{params}_G = (q, G_1, G_2, G_T, g_1, g_2, e)$$

[数134]

$$e: G_1 \times G_2 \rightarrow G_T$$

[0030] 双線形写像 e は、以下の双線形性と非退化性との2つの性質を有する。

(双線形性)

数135が成立する。

[数135]

$$e(g_1^Y, g_2^{\hat{Y}}) = e(g_1, g_2)^{Y\hat{Y}} \text{ for all } Y, \hat{Y} \in \mathbb{F}_q$$

(非退化性)

数136が成立する。ここで、数137は、群 G_T の単位元である。

[数136]

$$e(g_1, g_2) \neq 1_{G_T}$$

[数137]

$$1_{G_T}$$

[0031] 以下の説明では、 $G_{\text{BPG}}()$ を双線形群の生成アルゴリズムとする。つまり、 G_{BP}

G は、 param_G を生成するアルゴリズムである。

[0032] <双対ペアリングベクトル空間（以下、DPVS）>

数138に示すDPVSである param_V は、双線形群である param_G の直積によって構成される。 param_V は、素数 q と、要素毎に定義されたベクトル加算及びスカラー乗法の下での体 F_q 上の d 次元ベクトル空間 $V = G_1^d$ 及び d 次元ベクトル空間 $V^* = G_2^d$ と、ベクトル空間 V 及びベクトル空間 V^* の数139に示す標準基底 A_t と、数140に示すペアリング演算 e とを備える。

[数138]

$$\text{params}_V = (q, V, V^*, G_T, A, A^*, e)$$

[数139]

$$A = \{a^{(i)} = (\overbrace{1_{G_1}, \dots, 1_{G_1}}^{i-1}, g_1, \overbrace{1_{G_1}, \dots, 1_{G_1}}^{d-i})\}_{i \in [d]},$$

$$A^* = \{a^{*(i)} = (\overbrace{1_{G_2}, \dots, 1_{G_2}}^{i-1}, g_2, \overbrace{1_{G_2}, \dots, 1_{G_2}}^{d-i})\}_{i \in [d]}$$

[数140]

$$e: V \times V^* \rightarrow G_T$$

$$\text{defined by } e(v, w) = \prod_{i \in [d]} e(g_1^{v_i}, g_2^{w_i}) \in G_T$$

$$\text{for all } v = (g_1^{v_1}, \dots, g_1^{v_d}) \in V, w = (g_2^{w_1}, \dots, g_2^{w_d}) \in V^*$$

数139において、数141は単位元である。

[数141]

$$1_{G_1}, 1_{G_2}$$

[0033] param_V における写像 e は、以下の双線形性と非退化性との2つの性質を有する。

(双線形性)

数 1 4 2 が成立する。

[数142]

$$e(\Upsilon v, \hat{\Upsilon} w) = e(v, w) \Upsilon \hat{\Upsilon} \text{ for all } \Upsilon, \hat{\Upsilon} \in \mathbb{F}_q, v \in V, w \in V^*$$

(非退化性)

数 1 4 3 が成立する。

[数143]

$$\text{If } e(v, w) = 1_{G_T} \text{ for all } w \in V^*, \text{ then } v = \overbrace{1_{G_1}, \dots, 1_{G_1}}^d$$

v と w とを入れ替えても数 1 4 3 は成立する。

[0034] 数 1 4 4 に示すベクトル空間 V (又は、ベクトル空間 V^*) の基底 W と、ベクトル $v \mapsto \in \mathbb{F}_q^d$ とに対して、数 1 4 5 は、基底 W の要素とベクトル $v \mapsto$ の要素との線形結合によって構成されるベクトル空間 V (又は、ベクトル空間 V^*) のベクトルを示す。つまり、数 1 4 5 は、数 1 4 6 を示す。

[数144]

$$\mathbb{W} = \{w^{(1)}, \dots, w^{(d)}\} \text{ of } V(\text{or } V^*)$$

[数145]

$$(\vec{v})_{\mathbb{W}}$$

[数146]

$$(\vec{v})_{\mathbb{W}} = \sum_{i \in [d]} v_i w^{(i)} \in V(\text{or } V^*)$$

[0035] 数 1 4 7 に示すベクトルの集合について、数 1 4 8 は、数 1 4 7 に示すベクトルの集合によって張られたベクトル空間 V の部分空間を表す。

[数147]

$$\{v^{(i)}\}_{i \in [s]} \text{ of } V \text{ (or } V^*), s \in \mathbb{N}$$

[数148]

$$\text{SPAN} \langle v^{(i)} \mid i \in [s] \rangle$$

[0036] 以下の説明では、 $G_{\text{DPVS}}(1^\lambda, d)$ を DPVS の生成アルゴリズムとする。つまり、 G_{DPVS} は、単進符号のエンコーディングがされたセキュリティパラメータ 1^λ と、次元を示す自然数 d とを入力として、 d 次元ベクトル空間 V 及び d 次元ベクトル空間 V^* を伴う param_V を生成するアルゴリズムである。

[0037] 実施の形態 1 では、衝突困難性ハッシュ関数を用いて ABS を実現する。そこで、実施の形態 1 で用いる衝突困難性ハッシュ関数について説明する。

[0038] <衝突困難性ハッシュ関数>

双線形群の生成関数 G_{BPG} と、多項式 $\text{poly}(\cdot)$ とに関連付けられたハッシュ関数族 H は、 KGen アルゴリズムと、 $H^{(\lambda, \text{poly})}_{\text{kh}}$ アルゴリズムとの 2 つの多項式時間アルゴリズムから構成される。

[0039] KGen アルゴリズムは、ハッシュ鍵生成アルゴリズムである。 KGen アルゴリズムは、単進符号のエンコーディングがされたセキュリティパラメータ 1^λ を入力として、鍵空間 HK_λ からハッシュ鍵 hk をサンプリングする確率的アルゴリズムである。鍵空間 HK_λ は、 λ によってパラメータ化されたビット列上の確率的空間である。

[0040] $H^{(\lambda, \text{poly})}_{\text{kh}}$ アルゴリズムは、数 149 に示す写像を行う関数である。

[数149]

$$\mathcal{D} = \{0,1\}^{\text{poly}(\lambda)} \rightarrow \mathbb{F}_q \setminus \{0\}$$

つまり、 $H^{(\lambda, \text{poly})}_{\text{kh}}$ アルゴリズムは、単進符号のエンコーディングがされたセキュリティパラメータ 1^λ を入力として、 $\mathcal{D} = \{0, 1\}^{\text{poly}(\lambda)}$ の要

素から、0を除く体 F_q の要素への写像を行う確定的関数である。ここで、 q は、双線形群の生成関数 G_{BPG} の出力である $params_G$ の最初の要素である。

[0041] ***構成の説明***

以下の説明において、数150に示す q をある素数とし、数151を数152に示す全ての関数のクラスを示すものとする。数152において、 p は、体 F_q 上の多項式サイズのあるABPによって実現される任意の多項式である。

[数150]

$$q \in \mathbb{N}$$

[数151]

$$\mathcal{F}_{ABP}^{(q)}$$

[数152]

$$f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q \text{ for any } n = p(\lambda) \in \mathbb{N}$$

実施の形態1では、数153に示す述語族 $\mathcal{R}^{(q)}_{Z-ABP}$ に対するABS方式を説明する。

[数153]

$$\mathcal{R}_{Z-ABP}^{(q)} = \{\mathcal{R}_{Z-ABP}^{(q)}(f, \cdot): \mathbb{F}_q^n \rightarrow \{0,1\} \mid f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q \in \mathcal{F}_{ABP}^{(q)}\}$$

ここで、数154である。

[数154]

$$\begin{aligned} \mathcal{R}_{Z-ABP}^{(q)}(f, \vec{x}) &= 1 \text{ if } f(\vec{x}) = 0, \\ \mathcal{R}_{Z-ABP}^{(q)}(f, \vec{x}) &= 0 \text{ otherwise,} \\ \text{for all } f: \mathbb{F}_q^n &\rightarrow \mathbb{F}_q \in \mathcal{F}_{ABP}^{(q)}, \vec{x} \in \mathbb{F}_q^n \end{aligned}$$

[0042] A S Pの説明で述べた通り、数 1 5 5 に示すどんな関数 f の入力に対しても、数 1 5 6 に示す A S P のアクセスストラクチャ S を生成する多項式時間アルゴリズムが存在する。

[数155]

$$f: \mathbb{F}_q^n \rightarrow \mathbb{F}_q \in \mathcal{F}_{ABP}^{(q)}$$

[数156]

$$S = (U, \rho)$$

such that for any $\vec{x} \in \mathbb{F}_q^n$, it holds that

$$\mathcal{R}_{Z-ABP}^{(q)}(f, \vec{x}) = 1 \Leftrightarrow f(\vec{x}) = 0 \Leftrightarrow S \text{ accepts } \vec{x}$$

数 1 5 6 において、数 1 5 7 は、 $\mathcal{R}^{(q)}_{Z-ABP}(f, \vec{x})$ と、 $f(\vec{x}) = 0$ と、アクセスストラクチャ S が $\vec{x}$ を受理することとが同値であることを意味する。

[数157]

$$\mathcal{R}_{Z-ABP}^{(q)}(f, \vec{x}) = 1 \Leftrightarrow f(\vec{x}) = 0 \Leftrightarrow S \text{ accepts } \vec{x}$$

以下の説明では、述語 $\mathcal{R}^{(q)}_{Z-ABP}(f, \cdot) \in \mathcal{R}^{(q)}_{Z-ABP}$ は、多項式時間アルゴリズムによって計算された、対応する A S P 表現であるアクセスストラクチャ $S = (U, \rho)$ によって特定されるものとして説明する。

[0043] < A B S の構成 >

A B S 方式は、数 1 5 8 に示すメッセージ空間 M と、署名空間 Σ とを含むある述語族 $\mathcal{R}^{(q)}_{Z-ABP}$ に対する方式である。

[数158]

$$M \subseteq \{0,1\}^*$$

なお、数158における*は要素数が任意であることを意味する。

[0044] A B S方式は、S e t u pアルゴリズムと、K e y G e nアルゴリズムと、S i g nアルゴリズムと、V e r i f yアルゴリズムとを含む。

[0045] S e t u pアルゴリズムは、単進符号のエンコーディングがされたセキュリティパラメータ1^λを入力として、公開パラメータM P Kと、マスター秘密鍵M S Kとを出力する。

[0046] K e y G e nアルゴリズムは、公開パラメータM P Kと、マスター秘密鍵M S Kと、数159に示す属性ベクトル $x \rightarrow$ とを入力として、署名鍵S K ($x \rightarrow$)を出力する。

[数159]

$$\vec{x} \in \mathbb{F}_q^n \text{ for some } n = p(\lambda) \in \mathbb{N}$$

[0047] S i g nアルゴリズムは、公開パラメータM P Kと、数159に示す属性ベクトル $x \rightarrow$ と、属性ベクトル $x \rightarrow$ に対する署名鍵S K ($x \rightarrow$)と、署名ポリシー $R^{(q)}_{Z-ABP}(f, \cdot) : \mathbb{F}_q^n \rightarrow \{0, 1\} \in R^{(q)}_{Z-ABP}$ がA S P表現で表されたアクセス

ストラクチャ $S = (U, \rho)$ と、メッセージM S G $\in M$ とを入力として、署名s i g又は失敗を示す識別記号 $\perp$ を出力する。

[0048] V e r i f yアルゴリズムは、公開パラメータM P Kと、署名ポリシー $R^{(q)}_{Z-ABP}(f, \cdot) : \mathbb{F}_q^n \rightarrow \{0, 1\} \in R^{(q)}_{Z-ABP}$ がA S P表現で表されたアクセスストラクチャ $S = (U, \rho)$ と、メッセージM S G $\in M$ と署名s i g $\in \Sigma$ のペアとを入力として、1又は0を出力する。

[0049] <署名システム1の構成>

図1を参照して、実施の形態1に係る署名システム1の構成を説明する。

署名システム1は、セットアップ装置10と、鍵生成装置20と、署名装置30と、検証装置40とを備える。セットアップ装置10と、鍵生成装置20と、署名装置30と、検証装置40とは、コンピュータである。セットアップ装置10と、鍵生成装置20と、署名装置30と、検証装置40とは

、通信路を介して接続されている。

[0050] 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、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。

[0051] セットアップ装置10は、機能構成要素として、受付部111と、マスター鍵生成部112と、出力部113とを備える。セットアップ装置10の各機能構成要素の機能はソフトウェアにより実現される。

ストレージ13には、セットアップ装置10の各機能構成要素の機能を実現するプログラムが格納されている。このプログラムは、プロセッサ11によりメモリ12に読み込まれ、プロセッサ11によって実行される。これにより、セットアップ装置10の各機能構成要素の機能が実現される。

[0052] 図3を参照して、実施の形態1に係る鍵生成装置20の構成を説明する。

鍵生成装置20は、K e y G e n アルゴリズムを実行するコンピュータである。

鍵生成装置20は、プロセッサ21と、メモリ22と、ストレージ23と、通信インタフェース24とのハードウェアを備える。プロセッサ21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。

[0053] 鍵生成装置20は、機能構成要素として、取得部211と、署名鍵生成部212と、出力部213とを備える。鍵生成装置20の各機能構成要素の機能はソフトウェアにより実現される。

ストレージ23には、鍵生成装置20の各機能構成要素の機能を実現するプログラムが格納されている。このプログラムは、プロセッサ21によりメ

メモリ 22 に読み込まれ、プロセッサ 21 によって実行される。これにより、鍵生成装置 20 の各機能構成要素の機能が実現される。

[0054] 図 4 を参照して、実施の形態 1 に係る署名装置 30 の構成を説明する。

署名装置 30 は、S i g アルゴリズムを実行するコンピュータである。

署名装置 30 は、プロセッサ 31 と、メモリ 32 と、ストレージ 33 と、通信インタフェース 34 とのハードウェアを備える。プロセッサ 31 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。

[0055] 署名装置 30 は、機能構成要素として、取得部 311 と、署名部 312 と、出力部 31

3 とを備える。署名装置 30 の各機能構成要素の機能はソフトウェアにより実現される。

ストレージ 33 には、署名装置 30 の各機能構成要素の機能を実現するプログラムが格納されている。このプログラムは、プロセッサ 31 によりメモリ 32 に読み込まれ、プロセッサ 31 によって実行される。これにより、署名装置 30 の各機能構成要素の機能が実現される。

[0056] 図 5 を参照して、実施の形態 1 に係る検証装置 40 の構成を説明する。

検証装置 40 は、V e r i f y アルゴリズムを実行するコンピュータである。

検証装置 40 は、プロセッサ 41 と、メモリ 42 と、ストレージ 43 と、通信インタフェース 44 とのハードウェアを備える。プロセッサ 41 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。

[0057] 検証装置 40 は、機能構成要素として、取得部 411 と、検証データ生成部 412 と、検証部 413 とを備える。検証装置 40 の各機能構成要素の機能はソフトウェアにより実現される。

ストレージ 43 には、検証装置 40 の各機能構成要素の機能を実現するプログラムが格納されている。このプログラムは、プロセッサ 41 によりメモ

リ42に読み込まれ、プロセッサ41によって実行される。これにより、検証装置40の各機能構成要素の機能が実現される。

[0058] プロセッサ11, 21, 31, 41は、プロセッシングを行うIC (Integrated Circuit) である。プロセッサ11, 21, 31, 41は、具体例としては、CPU (Central Processing Unit)、DSP (Digital Signal Processor)、GPU (Graphics Processing Unit) である。

[0059] メモリ12, 22, 32, 42は、データを一時的に記憶する記憶装置である。メモリ12, 22, 32, 42は、具体例としては、SRAM (Static Random Access Memory)、DRAM (Dynamic Random Access Memory) である。

[0060] ストレージ13, 23, 33, 43は、データを保管する記憶装置である。ストレージ13, 23, 33, 43は、具体例としては、HDD (Hard Disk Drive) である。また、ストレージ13, 23, 33, 43は、SD (登録商標, Secure Digital) メモリカード、CF (CompactFlash, 登録商標)、NANDフラッシュ、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ (登録商標) ディスク、DVD (Digital Versatile Disk) といった可搬記録媒体であってもよい。

[0061] 通信インタフェース14, 24, 34, 44は、外部の装置と通信するためのインタフェースである。通信インタフェース14, 24, 34, 44は、具体例としては、Ethernet (登録商標)、USB (Universal Serial Bus)、HDMI (登録商標, High-Definition Multimedia Interface) のポートである。

[0062] 図2では、プロセッサ11は、1つだけ示されていた。しかし、プロセッサ11は、複数であってもよく、複数のプロセッサ11が、各機能を実現す

るプログラムを連携して実行してもよい。同様に、プロセッサ 2 1, 3 1, 4 1 は、複数であってもよく、複数のプロセッサ 2 1, 3 1, 4 1 が、各機能を実現するプログラムを連携して実行してもよい。

[0063] ***動作の説明***

図 6 から図 9 を参照して、実施の形態 1 に係る署名システム 1 の動作を説明する。

以下の説明では、A S P の記述における関数 ρ は、単射である必要はない。そのため、以下に説明する A B S 方式は、署名ポリシーにおける無制限な属性のマルチユースをサポートする。無制限とは、公開パラメータ M P K によって、属性の数が制限されないという意味である。また、マルチユースとは、同じ属性を複数個所で使うことが可能であるという意味である。

[0064] 図 6 を参照して、実施の形態 1 に係るセットアップ装置 1 0 の動作を説明する。

実施の形態 1 に係るセットアップ装置 1 0 の動作は、実施の形態 1 に係るセットアップ方法に相当する。また、実施の形態 1 に係るセットアップ装置 1 0 の動作は、実施の形態 1 に係るセットアッププログラムの処理に相当する。

[0065] (ステップ S 1 1 : 受付処理)

受付部 1 1 1 は、単進符号のエンコーディングがされたセキュリティパラメータ 1^λ の入力を受け付ける。受付部 1 1 1 は、セキュリティパラメータ 1^λ をメモリ 1 2 に書き込む。

[0066] (ステップ S 1 2 : 基底生成処理)

マスター鍵生成部 1 1 2 は、ステップ S 1 1 で受付されたセキュリティパラメータ 1^λ を入力として、 $p a r a m s$ 及び正規直交な双対基底 $\{B_\ell, B_\ell^*\}_{\ell \in [0, 2]}$ を生成する。

具体的には、マスター鍵生成部 1 1 2 は、セキュリティパラメータ λ をメモリ 1 2 から読み出す。マスター鍵生成部 1 1 2 は、 $N=2$ 、 $d_0=4$ 、 $d_1=14$ 、 $d_2=8$ として、数 1 6 0 に示すアルゴリズム G_{OB} を実行して、 $p a$

params 及び双対基底 $\{B_\iota, B^*_\iota\}_{\iota \in [0, 2]}$ を生成する。マスター鍵生成部 112 は、params 及び双対基底 $\{B_\iota, B^*_\iota\}_{\iota \in [0, 2]}$ をメモリ 12 に書き込む。

[数160]

$G_{OB}(N, (d_0, \dots, d_N)):$

$\text{params}_{\mathbb{G}} = (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e) \xleftarrow{R} G_{BPG}(),$

$\psi \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, g_T = e(g_1, g_2)^\psi,$

for $\iota \in [0, N]$

$\text{params}_{\mathbb{V}_\iota} = (q, \mathbb{V}_\iota, \mathbb{V}_\iota^*, \mathbb{G}_T, A_\iota, A_\iota^*, e)$

$\xleftarrow{R} G_{DPVS}(d_\iota, \text{params}_{\mathbb{G}}),$

$B^{(\iota)} = (b_{k,i}^{(\iota)}) \xleftarrow{U} GL(d_\iota, \mathbb{F}_q),$

$B^{*(\iota)} = (b_{k,i}^{*(\iota)}) = \psi((B^{(\iota)})^{-1})^T,$

for all $k \in [d_\iota],$

let $\vec{b}^{(\iota,k)}$ and $\vec{b}^{*(\iota,k)}$ represent the k^{th} rows of $B^{(\iota)}$ and $B^{*(\iota)}$,

$b^{(\iota,k)} = (\vec{b}^{(\iota,k)})_{A_\iota}, b^{*(\iota,k)} = (\vec{b}^{*(\iota,k)})_{A_\iota^*}$ for $k \in [d_\iota],$

$\mathbb{B}_\iota = \{b^{(\iota,1)}, \dots, b^{(\iota,d_\iota)}\}, \mathbb{B}_\iota^* = \{b^{*(\iota,1)}, \dots, b^{*(\iota,d_\iota)}\},$

$\text{params} = (\{\text{params}_{\mathbb{V}_\iota}\}_{\iota \in [0, N]}, g_T),$

return $(\text{params}, \{\mathbb{B}_\iota, \mathbb{B}_\iota^*\}_{\iota \in [0, N]}).$

[0067] (ステップS13: 部分基底生成処理)

マスター鍵生成部 112 は、ステップS12で生成された双対基底 $\{B_\iota, B^*_\iota\}_{\iota \in [0, 2]}$ から、 $\iota \in [0, 2]$ の各整数 ι について、部分基底 $B^\wedge_\iota$ 及び部分基底 $B^{\wedge*}_\iota$ を生成する。

具体的には、マスター鍵生成部 112 は、params 及び双対基底 $\{B_\iota, B^*_\iota\}_{\iota \in [0, 2]}$ をメモリ 12 から読み出す。マスター鍵生成部 112 は、数 161 に示すように、 $\iota \in [0, 2]$ の各整数 ι について、部分基底 $B^\wedge_\iota$ 及び部分基底 $B^{\wedge*}_\iota$ を生成する。

[数161]

$$\begin{aligned}
\hat{\mathcal{B}}_0 &= \{b^{(0,1)}, b^{(0,4)}\}, \\
\hat{\mathcal{B}}_0^* &= \{b^{*(0,3)}\}, \\
\hat{\mathcal{B}}_1 &= \{b^{(1,1)}, \dots, b^{(1,4)}, b^{(1,13)}, b^{(1,14)}\}, \\
\hat{\mathcal{B}}_1^* &= \{b^{*(1,1)}, \dots, b^{*(1,4)}, b^{*(1,11)}, b^{*(1,12)}\}, \\
\hat{\mathcal{B}}_2 &= \{b^{(2,1)}, b^{(2,2)}, b^{(2,7)}, b^{(2,8)}\}, \\
\hat{\mathcal{B}}_2^* &= \{b^{*(2,1)}, b^{*(2,2)}, b^{*(2,5)}, b^{*(2,6)}\}
\end{aligned}$$

[0068] (ステップS 1 4 : ハッシュ鍵生成処理)

マスター鍵生成部 1 1 2 は、数 1 6 2 に示すように、K G e n アルゴリズムにより、ハッシュ鍵 hk をサンプリングする。

[数162]

$$hk \xleftarrow{R} KGen()$$

ここで、K G e n アルゴリズムは、双線形群の生成関数 G_{BPG} と、多項式 $poly(\cdot)$ とに関連付けられたハッシュ関数族 H に対するアルゴリズムである。多項式 $poly(\lambda)$ は、メッセージ空間 M に属するメッセージと、述語族 $R^{(q)}_{Z-ABP}$ における署名ポリシー述語を表す A S P の 2 値表現とを連接することによって形成されたビット列の長さを表す。

[0069] (ステップS 1 5 : マスター鍵設定処理)

マスター鍵生成部 1 1 2 は、ステップS 1 2 で生成された $params$ と、ステップS 1 3 で生成された $\iota \in [0, 2]$ の各整数 ι についての部分基底 $B^\wedge_\iota$ 及び部分基底 $B^{\wedge*}_\iota$ と、ステップS 1 4 で生成されたハッシュ鍵 hk とを公開パラメータ MPK として設定する。また、マスター鍵生成部 1 1 2 は、基底ベクトル $b^{*(0,1)}$ をマスター秘密鍵 MSK として設定する。

そして、マスター鍵生成部 1 1 2 は、公開パラメータ MPK 及びマスター秘密鍵 MSK をメモリ 1 2 に書き込む。

[0070] (ステップS 1 6 : 出力処理)

出力部 113 は、ステップ S15 で設定された公開パラメータ MPK 及びマスター秘密鍵 MSK を出力する。

具体的には、出力部 113 は、公開パラメータ MPK 及びマスター秘密鍵 MSK をメモリ 12 から読み出す。出力部 113 は、公開パラメータ MPK を公開用のサーバに送信するといった方法により、公開する。これにより、鍵生成装置 20 と署名装置 30 と検証装置 40 とは、公開パラメータ MPK を取得可能になる。また、出力部 113 は、マスター秘密鍵 MSK を秘密裡に鍵生成装置 20 に送信する。秘密裡に送信するとは、既存の暗号化方式で暗号化した上で送信するといった意味である。

[0071] つまり、セットアップ装置 10 は、数 163 に示す Setup アルゴリズムを実行する。

[数163]

Setup():

1. $(\text{params}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t \in [0,2]}) \xleftarrow{R} G_{OB}(2, (4, 14, 8)),$
2. $\hat{\mathbb{B}}_0 = \{b^{(0,1)}, b^{(0,4)}\},$
 $\hat{\mathbb{B}}_0^* = \{b^{*(0,3)}\},$
 $\hat{\mathbb{B}}_1 = \{b^{(1,1)}, \dots, b^{(1,4)}, b^{(1,13)}, b^{(1,14)}\},$
 $\hat{\mathbb{B}}_1^* = \{b^{*(1,1)}, \dots, b^{*(1,4)}, b^{*(1,11)}, b^{*(1,12)}\},$
 $\hat{\mathbb{B}}_2 = \{b^{(2,1)}, b^{(2,2)}, b^{(2,7)}, b^{(2,8)}\},$
 $\hat{\mathbb{B}}_2^* = \{b^{*(2,1)}, b^{*(2,2)}, b^{*(2,5)}, b^{*(2,6)}\},$
3. $hk \xleftarrow{R} KGen(),$
4. $\text{output } MPK = (hk, \text{params}, \{\hat{\mathbb{B}}_t, \hat{\mathbb{B}}_t^*\}_{t \in [0,2]}),$
 $MSK = b^{*(0,1)}.$

[0072] 図 7 を参照して、実施の形態 1 に係る鍵生成装置 20 の動作を説明する。

実施の形態 1 に係る鍵生成装置 20 の動作は、実施の形態 1 に係る鍵生成方法に相当する。また、実施の形態 1 に係る鍵生成装置 20 の動作は、実施の形態 1 に係る鍵生成プログラムの処理に相当する。

[0073] (ステップS 2 1 : 取得処理)

取得部2 1 1は、ステップS 1 6で出力された公開パラメータMP K及びマスター秘密鍵MS Kを取得する。また、取得部2 1 1は、属性ベクトル $x \rightarrow \in F^{n_q}$ を取得する。ここでは、属性ベクトル $x \rightarrow$ は、生成される署名鍵SK ($x \rightarrow$)のユーザの属性である。なお、属性ベクトル $x \rightarrow \in F^{n_q}$ における n は、属性ベクトル $x \rightarrow$ の要素数を表している。つまり、属性ベクトル $x \rightarrow = (x_1, \dots, x_n)$ である。 n は1以上の整数である。

取得部2 1 1は、公開パラメータMP K及びマスター秘密鍵MS Kと、属性ベクトル $x \rightarrow$ とをメモリ2 2に書き込む。

[0074] (ステップS 2 2 : 署名鍵生成処理)

署名鍵生成部2 1 2は、数1 6 4に示すように、乱数 ω と乱数 ϕ_0 とをサンプリングし、要素 $k^{*(0)}$ を生成する。

[数164]

$$\omega \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \phi_0 \xleftarrow{U} \mathbb{F}_q, \\ k^{*(0)} = (\omega, 0, \phi_0, 0)_{\mathbb{B}_0^*}$$

[0075] 署名鍵生成部2 1 2は、 $i \in [n]$ の各整数 i について、数1 6 5に示すように、乱数

σ_i と乱数 $\phi^{*(i)}$ とをサンプリングし、要素 $k^{*(i)}$ を生成する。

[数165]

$$\sigma_i \xleftarrow{U} \mathbb{F}_q, \vec{\phi}^{*(i)} \xleftarrow{U} \mathbb{F}_q^2, \\ k^{*(i)} = (\sigma_i(1, i), \omega(1, x_i), \vec{0}^6, \vec{\phi}^{*(i)}, \vec{0}^2)_{\mathbb{B}_1^*}$$

[0076] ここで、基底 $B^*_{i_1}$ の基底ベクトル $b^{*(1, 1)}$ 及び基底ベクトル $b^{*(1, 2)}$ は、インデックス部である。そして、インデックス部に係数として設定された $\sigma_i(1, i)$ は、属性ベクトル $x \rightarrow$ の要素 x_i に応じたインデックス情報 l^* である。インデックス情報 l^* は、後述するVerifyアルゴリズムにおいて用いられる、対応するインデックス情報 l との要素毎の内積の和が0になる。

[0077] 署名鍵生成部212は、数166に示すように、乱数 $\phi \rightarrow (n+1, 1)$ 及び乱数 $\phi \rightarrow (n+1, 2)$ をサンプリングし、要素 $k^* (n+1, 1)$ 及び要素 $k^* (n+1, 2)$ を生成する。

[数166]

$$\begin{aligned}\vec{\phi}^{(n+1,1)}, \vec{\phi}^{(n+1,2)} &\xleftarrow{U} \mathbb{F}_q^2, \\ k^{*(n+1,1)} &= (\omega(1,0), \vec{0}^2, \vec{\phi}^{(n+1,1)}, \vec{0}^2)_{\mathbb{B}_2^*}, \\ k^{*(n+1,2)} &= (\omega(0,1), \vec{0}^2, \vec{\phi}^{(n+1,2)}, \vec{0}^2)_{\mathbb{B}_2^*},\end{aligned}$$

[0078] 署名鍵生成部212は、要素 $k^* (0)$ と、 $\iota \in [n]$ の各整数 ι についての要素 $k^* (\iota)$ と、要素 $k^* (n+1, 1)$ 及び要素 $k^* (n+1, 2)$ とを署名鍵 $SK (x \rightarrow)$ としてメモリ22に書き込む。

[0079] (ステップS23：出力処理)

出力部213は、ステップS22で生成された署名鍵 $SK (x \rightarrow)$ を出力する。

具体的には、出力部213は、署名鍵 $SK (x \rightarrow)$ をメモリ22から読み出す。出力部213は、署名鍵 $SK (x \rightarrow)$ を秘密裡に署名装置30に送信する。

[0080] つまり、鍵生成装置20は、数167に示すKey Genアルゴリズムを実行する。

[数167]

$$\text{KeyGen}(\text{MPK}, \text{MSK}, \vec{x}):$$

1. $\omega \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \phi_0 \xleftarrow{U} \mathbb{F}_q,$
 $k^*(0) = (\omega, 0, \phi_0, 0)_{\mathbb{B}_0^*},$
2. for $\iota \in [n]$
 $\sigma_\iota \xleftarrow{U} \mathbb{F}_q, \vec{\phi}(\iota) \xleftarrow{U} \mathbb{F}_q^2,$
 $k^*(\iota) = (\sigma_\iota(1, \iota), \omega(1, x_\iota), \vec{0}^6, \vec{\phi}(\iota), \vec{0}^2)_{\mathbb{B}_1^*},$
3. $\vec{\phi}^{(n+1,1)}, \vec{\phi}^{(n+1,2)} \xleftarrow{U} \mathbb{F}_q^2,$
 $k^*(n+1,1) = (\omega(1, 0), \vec{0}^2, \vec{\phi}^{(n+1,1)}, \vec{0}^2)_{\mathbb{B}_2^*},$
 $k^*(n+1,2) = (\omega(0, 1), \vec{0}^2, \vec{\phi}^{(n+1,2)}, \vec{0}^2)_{\mathbb{B}_2^*},$
4. output $SK(\vec{x}) = (k^*(0), \dots, k^*(n), k^*(n+1,1), k^*(n+1,2)).$

[0081] 図8を参照して、実施の形態1に係る署名装置30の動作を説明する。

実施の形態1に係る署名装置30の動作は、実施の形態1に係る署名方法に相当する。また、実施の形態1に係る署名装置30の動作は、実施の形態1に係る署名プログラムの処理に相当する。

[0082] (ステップS31：取得処理)

取得部311は、ステップS16で出力された公開パラメータMPKを取得する。また、取得部311は、ステップS23で出力された署名鍵SK ($x \mapsto$) を取得する。

また、取得部311は、ユーザの属性ベクトル $x \mapsto \in \mathbb{F}_{q^n}$ と、署名ポリシー $R^{(q)}_{Z-ABP}(f, \cdot) : \mathbb{F}_{q^n} \rightarrow \{0, 1\} \in R^{(q)}_{Z-ABP}$ がASP表現で表されたアクセスストラクチャSと、メッセージ $MSG \in M$ とを取得する。ここで、アクセスストラクチャSは、数168に示す通りである。

[数168]

$$S = (U = \{\vec{y}^{(j)}, \vec{z}^{(j)}\}_{j \in [m]} \subset (\mathbb{F}_q^L)^2, \rho : [m] \rightarrow [n])$$

L は、ベクトル $y^{(j)}$ 及びベクトル $z^{(j)}$ の要素数であり、1 以上の整数である。

取得部 311 は、公開パラメータ MPK と、署名鍵 $SK(x)$ と、ユーザの属性ベクトル $x \in F_q^n$ と、アクセスストラクチャ S と、メッセージ MSG とをメモリ 32 に書き込む。

[0083] (ステップ S32 : 判定処理)

署名部 312 は、アクセスストラクチャ S が属性ベクトル x を受理するかどうかを判定する。

署名部 312 は、受理する場合には、処理をステップ S33 に進める。一方、署名部 3

12 は、受理しない場合には、失敗を示す識別記号 $\perp$ を出力して、処理を終了する。

[0084] (ステップ S33 : 変数計算処理)

署名部 312 は、数 169 に示すスカラー $(\Omega_j)_{j \in [m]} \in F_q^m$ を計算する。

[数169]

$$\vec{e}(L, L) = \sum_{j \in [m]} \Omega_j (x_{\rho(j)} \vec{y}^{(j)} + \vec{z}^{(j)})$$

ここで、数 127 である場合に限り、数 128 に示す属性ベクトル x はアクセスストラクチャ S を満たす。そのため、数 169 に示すスカラー $(\Omega_j)_{j \in [m]} \in F_q^m$ は存在し、計算可能である。

[0085] 署名部 312 は、数 170 に示す乱数 ξ と、乱数 $(\Omega'_j)_{j \in [m]} \in F_q^m$ 及び乱数 $(\Omega''_j)_{j \in [m]} \in F_q^m$ とをサンプリングする。

[数170]

$$\begin{aligned} \xi &\xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \\ ((\Omega'_j)_{j \in [m]}, (\Omega''_j)_{j \in [m]}) &\xleftarrow{U} (\mathbb{F}_q^m)^2 \\ \text{such that } \sum_{j \in [m]} (\Omega'_j \bar{y}^{(j)} + \Omega''_j \bar{z}^{(j)}) &= \vec{0}^L \end{aligned}$$

[0086] 署名部312は、スカラー $(\Omega_j)_{j \in [m]}$ と、乱数 ξ と、乱数 $(\Omega'_j)_{j \in [m]}$ 及び乱数 $(\Omega''_j)_{j \in [m]}$ とをメモリ32に書き込む。

[0087] (ステップS34：署名要素生成処理)

署名部312は、数171に示すように、乱数 $r^{*(0)}$ をサンプリングし、要素 $s^{*(0)}$ を生成する。

[数171]

$$\begin{aligned} r^{*(0)} &\xleftarrow{U} \text{SPAN} \langle b^{*(0,3)} \rangle, \\ s^{*(0)} &= \xi k^{*(0)} + r^{*(0)} \end{aligned}$$

乱数 ξ と乱数 $r^{*(0)}$ とにより、署名鍵 $SK(x \rightarrow)$ の要素 $k^{*(0)}$ に設定された乱数 ω 及び乱数 ϕ_0 が隠蔽される。

[0088] 署名部312は、 $j \in [m]$ の各整数 j について、数172に示すように、乱数 σ'_j と、乱数 $r^{*(j)}$ とをサンプリングし、要素 $s^{*(j)}$ を生成する。

[数172]

$$\begin{aligned} \sigma'_j &\xleftarrow{U} \mathbb{F}_q, r^{*(j)} \xleftarrow{U} \text{SPAN} \langle b^{*(1,1)}, b^{*(1,2)} \rangle, \\ s^{*(j)} &= \xi \Omega_j k^{*(\rho(j))} + \sigma'_j (b^{*(1,1)} + \rho(j) b^{*(1,2)}) \\ &\quad + \Omega''_j b^{*(1,3)} + \Omega'_j b^{*(1,4)} + r^{*(j)} \end{aligned}$$

ここで、乱数 ξ とスカラー Ω_j とにより、署名鍵 $SK(x \rightarrow)$ の要素 $k^{*(\rho(j))}$ に設定された属性ベクトル $x \rightarrow$ の要素が隠蔽される。乱数 Ω'_j により $\Omega_j x_{\rho(j)}$ が隠蔽される。乱数 Ω''_j により乱数 Ω'_j が隠蔽される。

また、乱数 σ'_j により、署名鍵 $SK(x \rightarrow)$ の要素 $k^{*(\iota)}$ に設定されたインデックス情報 l^* が隠蔽される。乱数 $r^{*(j)}$ により、署名鍵 $SK(x \rightarrow)$ の要素 $k^{*(\iota)}$ に設定された乱数 $\phi \rightarrow (\iota)$ が隠蔽される。

[0089] 署名部 312 は、数 173 に示すように、乱数 $r^{*(m+1)}$ をサンプリングし、要素 $s^{*(m+1)}$ を生成する。

[数173]

$$r^{*(m+1)} \xleftarrow{U} SPAN \langle b^{*(2,5)}, b^{*(2,6)} \rangle,$$

$$s^{*(m+1)} = \xi(k^{*(n+1,1)} + H_{hk}^{(\lambda, poly)}(MSG \parallel S)k^{*(n+1,2)}) + r^{*(m+1)}$$

ここで、乱数 ξ と乱数 $r^{*(m+1)}$ とにより、署名鍵 $SK(x \rightarrow)$ の要素 $k^{*(n+1,1)}$ 及び要素 $k^{*(n+1,2)}$ に設定された乱数 ω と乱数 $\phi \rightarrow (n+1,1)$ と乱数 $\phi \rightarrow (n+1,2)$ とが隠蔽される。

[0090] 署名部 312 は、要素 $s^{*(0)}$ と、 $j \in [m]$ の各整数 j についての要素 $s^{*(j)}$ と、要素 $s^{*(m+1)}$ とを署名 sig としてメモリ 32 に書き込む。

[0091] (ステップ S35 : 出力処理)

出力部 313 は、ステップ S31 で取得されたメッセージ MSG と、ステップ S34 で生成された署名 sig とのペアを出力する。

具体的には、出力部 313 は、メッセージ MSG 及び署名 sig をメモリ 32 から読み出す。出力部 313 は、メッセージ MSG 及び署名 sig を検証装置 40 に送信する。

[0092] つまり、署名装置 30 は、数 174 に示す Sig アルゴリズムを実行する。

[数174]

$Sig(MPK, \vec{x}, SK(\vec{x}), S, MSG):$

if S does not accept $\vec{x}$, it outputs $\perp$,

Otherwise, i.e., if S accepts $\vec{x}$, it operates as follows:

1. computes $(\Omega_j)_{j \in [m]} \in \mathbb{F}_q^m$

$$\text{such that } \vec{e}^{(L,L)} = \sum_{j \in [m]} \Omega_j (x_{\rho(j)} \vec{y}^{(j)} + \vec{z}^{(j)}),$$

2. $\xi \xleftarrow{U} \mathbb{F}_q \setminus \{0\}$,

$$((\Omega'_j)_{j \in [m]}, (\Omega''_j)_{j \in [m]}) \xleftarrow{U} (\mathbb{F}_q^m)^2$$

$$\text{such that } \sum_{j \in [m]} (\Omega'_j \vec{y}^{(j)} + \Omega''_j \vec{z}^{(j)}) = \vec{0}^L,$$

3. $r^{*(0)} \xleftarrow{U} SPAN \langle b^{*(0,3)} \rangle$,

$$s^{*(0)} = \xi k^{*(0)} + r^{*(0)},$$

4. for $j \in [m]$

$$\sigma'_j \xleftarrow{U} \mathbb{F}_q, r^{*(j)} \xleftarrow{U} SPAN \langle b^{*(1,1)}, b^{*(1,2)} \rangle,$$

$$s^{*(j)} = \xi \Omega_j k^{*(\rho(j))} + \sigma'_j (b^{*(1,1)} + \rho(j) b^{*(1,2)}) \\ + \Omega''_j b^{*(1,3)} + \Omega'_j b^{*(1,4)} + r^{*(j)},$$

5. $r^{*(m+1)} \xleftarrow{U} SPAN \langle b^{*(2,5)}, b^{*(2,6)} \rangle$,

$$s^{*(m+1)} = \xi (k^{*(n+1,1)} + H_{hk}^{(\lambda, poly)}(MSG \parallel S) k^{*(n+1,2)}) + r^{*(m+1)},$$

6. output $sig = (s^{*(0)}, \dots, s^{*(m+1)})$.

[0093] 図9を参照して、実施の形態1に係る検証装置40の動作を説明する。

実施の形態1に係る検証装置40の動作は、実施の形態1に係る検証方法に相当する。また、実施の形態1に係る検証装置40の動作は、実施の形態1に係る検証プログラムの処理に相当する。

[0094] (ステップS41：取得処理)

取得部411は、ステップS16で出力された公開パラメータMPKを取得する。また、取得部411は、ステップS35で出力されたメッセージM

S G 及び署名 $s_i g$ のペアを取得する。また、取得部 4 1 1 は、署名ポリシ
ー $R^{(q)}_{Z-ABP}(f, \cdot) : F^n_q \rightarrow \{0, 1\} \in R^{(q)}_{Z-ABP}$ が A S P 表現で
表されたアクセスストラクチャ S を

取得する。

取得部 4 1 1 は、公開パラメータ M P K と、メッセージ M S G 及び署名 $s_i g$ のペアと、アクセスストラクチャ S とをメモリ 4 2 に書き込む。

[0095] (ステップ S 4 2 : 検証データ生成処理)

検証データ生成部 4 1 2 は、数 1 7 5 に示すように、乱数 u をサンプリン
グし、 $j \in [m]$ の各整数 j について検証情報である変数 s_j 及び変数 s'_j
を生成する。

[数175]

$$\begin{aligned} \vec{u} &= (u_1, \dots, u_L) \xleftarrow{U} \mathbb{F}_q^L, \\ \text{for } j &\in [m] \\ s_j &= \vec{u} \cdot \vec{y}(j), \\ s'_j &= \vec{u} \cdot \vec{z}(j) \end{aligned}$$

[0096] 検証データ生成部 4 1 2 は、数 1 7 6 に示すように、乱数 u 及び乱数 η_0 を
サンプリングし、要素 $c^{(0)}$ を生成する。

[数176]

$$\begin{aligned} u, \eta_0 &\xleftarrow{U} \mathbb{F}_q, \\ c^{(0)} &= (-u - u_L, 0, 0, \eta_0)_{\mathbb{B}_0} \end{aligned}$$

[0097] 検証データ生成部 4 1 2 は、 $j \in [m]$ の各整数 j について以下を実行す
る。

まず、検証データ生成部 4 1 2 は、対象の整数 j について、数 1 7 7 が成
立するか否かを判定する。

[数177]

$$s^{*(j)} \notin V_1^*$$

検証データ生成部412は、成立する場合には、署名 $s_i g$ の正当性が確認できないことを示す0を出力して処理を終了する。一方、検証データ生成部412は、成立しない場合には、対象の整数 j について、数178に示すように、乱数 μ_j 及び乱数 $\vec{\eta}^{(j)}$ をサンプリングし、要素 $c^{(j)}$ を生成する。

[数178]

$$\begin{aligned} \mu_j &\xleftarrow{U} \mathbb{F}_q, \quad \vec{\eta}^{(j)} \xleftarrow{U} \mathbb{F}_q^2, \\ c^{(j)} &= (\mu_j(\rho(j), -1), (s'_j, s_j), \vec{0}^6, \vec{0}^2, \vec{\eta}^{(j)})_{\mathbb{B}_1} \end{aligned}$$

[0098] ここで、基底 B_1 の基底ベクトル $b^{(1, 1)}$ 及び基底ベクトル $b^{(1, 2)}$ は、インデックス部である。基底 B_1 の基底ベクトル $b^{(1, 1)}$ 及び基底ベクトル $b^{(1, 2)}$ は、基底 B^*_1 の基底ベクトル $b^{*(1, 1)}$ 及び基底ベクトル $b^{*(1, 2)}$ に対応する基底ベクトルである。対応する基底ベクトルとは、ペアリング演算で内積が計算される基底ベクトルであるという意味である。

そして、インデックス部に係数として設定された $\mu_j(\rho(j), -1)$ は、インデックス情報 l である。インデックス情報 l は、署名鍵 $SK(x)$ で用いられた、対応するインデックス情報 l^* との要素毎の内積の和が0になる。インデックス情報が対応するとは、 l と $\rho(j)$ とが対応しているという意味であり、 $l = \rho(j)$ という意味である。

具体的には、インデックス情報 l^* は $\sigma_l(1, l)$ であり、インデックス情報 l は $\mu_j(\rho(j), -1)$ である。 $l = \rho(j)$ であるため、 $\sigma_l \mu_j(1 \cdot \rho(j) - 1 \cdot l) = \sigma_l \mu_j(1 \cdot l - 1 \cdot l) = 0$ である。

[0099] 検証データ生成部412は、数179に示すように、乱数 κ 及び乱数 $\vec{\eta}^{(m+1)}$ をサンプリングし、要素 $c^{(m+1)}$ を生成する。

[数179]

$$\kappa \xleftarrow{U} \mathbb{F}_q, \bar{\eta}^{(m+1)} \xleftarrow{U} \mathbb{F}_q^2,$$

$$c^{(m+1)} = ((u - \kappa H_{hk}^{(\lambda, poly)}(MSG \| S), \kappa), \vec{0}^2, \vec{0}^2, \bar{\eta}^{(m+1)})_{\mathbb{B}_2}$$

[0100] (ステップS43: 第1検証処理)

検証部413は、数180が成立するか否かを判定する。

[数180]

$$e(b^{(0,1)}, s^{*(0)}) = 1_{\mathbb{G}_T}$$

検証部413は、成立する場合には、署名sigの正当性が確認できないことを示す0を出力して処理を終了する。一方、検証部413は、成立しない場合には、処理をステップS44に進める。

[0101] (ステップS44: 第2検証処理)

検証部413は、数181が成立するか否かを判定する。

[数181]

$$\prod_{j \in [0, m+1]} e(c^{(j)}, s^{*(j)}) = 1_{\mathbb{G}_T}$$

検証部413は、成立する場合には、署名sigの正当性が確認できたことを示す1を出力して処理を終了する。一方、検証部413は、成立しない場合には、署名sigの正当性が確認できないことを示す0を出力して処理を終了する。

[0102] 数182に示すように、署名sigが正当である場合には、数181が成立する。

[数182]

$$\begin{aligned}
& \prod_{j \in [0, m+1]} e(c(j), s^*(j)) \\
&= e(c(0), k^*(0))^\xi \cdot \prod_{j \in [m]} e(c(j), k^*(\rho(j)))^{\xi \Omega_j} \cdot \\
& \quad \prod_{j \in [m]} e(c(j), b^*(1,3))^{\Omega_j''} e(c(j), b^*(1,4))^{\Omega_j'} \cdot \\
& \quad [e(c(m+1), k^*(n+1,1)) \cdot e(c(m+1), k^*(n+1,2)) H_{hk}^{(\lambda, poly)}(MSG \| S)]^\xi \\
&= g_T^{\xi \omega(-u-u_L)} \cdot \prod_{j \in [m]} g_T^{\xi \omega \Omega_j (x_{\rho(j)} s_j + s_j')} \\
& \quad \cdot \prod_{j \in [m]} g_T^{(\Omega_j' s_j + \Omega_j'' s_j')} \cdot g_T^{\xi \omega u} \\
&= g_T^{\xi \omega(-u-u_L)} \cdot g_T^{\xi \omega(\vec{u} \cdot \sum_{j \in [m]} \Omega_j (x_{\rho(j)} \vec{y}^{(j)} + \vec{z}^{(j)}))} \\
& \quad \cdot g_T^{\vec{u} \cdot \sum_{j \in [m]} (\Omega_j' \vec{y}^{(j)} + \Omega_j'' \vec{z}^{(j)})} \cdot g_T^{\xi \omega u} \\
&= g_T^{\xi \omega(-u-u_L)} \cdot g_T^{\xi \omega(\vec{u} \cdot \vec{e}^{(L,L)})} \cdot g_T^{\vec{u} \cdot \vec{0}^L} \cdot g_T^{\xi \omega u} \\
&= g_T^{\xi \omega(-u-u_L)} \cdot g_T^{\xi \omega u_L} \cdot 1_{G_T} \cdot g_T^{\xi \omega u} \\
&= 1_{G_T}
\end{aligned}$$

[0103] つまり、検証装置40は、数183に示すVerifyアルゴリズムを実行する。

[数183]

$Verify(MPK, \mathcal{S}, (MSG, sig)):$

- 1.(a) $\vec{u} = (u_1, \dots, u_L) \xleftarrow{U} \mathbb{F}_q^L$,
for $j \in [m]$ $s_j = \vec{u} \cdot \vec{y}(j)$, $s'_j = \vec{u} \cdot \vec{z}(j)$,
(b) $u, \eta_0 \xleftarrow{U} \mathbb{F}_q$, $c^{(0)} = (-u - u_L, 0, 0, \eta_0)_{\mathbb{B}_0}$,
(c) for $j \in [m]$ if $s^{*(j)} \notin \mathbb{V}_1^*$ then it outputs 0. Otherwise,
 $\mu_j \xleftarrow{U} \mathbb{F}_q$, $\vec{\eta}(j) \xleftarrow{U} \mathbb{F}_q^2$,
 $c^{(j)} = (\mu_j(\rho(j), -1), (s'_j, s_j), \vec{0}^6, \vec{0}^2, \vec{\eta}(j))_{\mathbb{B}_1}$
(d) $\kappa \xleftarrow{U} \mathbb{F}_q$, $\vec{\eta}^{(m+1)} \xleftarrow{U} \mathbb{F}_q^2$,
 $c^{(m+1)} = ((u - \kappa H_{hk}^{(\lambda, poly)}(MSG \parallel \mathcal{S}), \kappa), \vec{0}^2, \vec{0}^2, \vec{\eta}^{(m+1)})_{\mathbb{B}_2}$
2. It outputs 0 if $e(b^{(0,1)}, s^{*(0)}) = 1_{\mathbb{G}_T}$,
3. It outputs 1 if $\prod_{j \in [0, m+1]} e(c^{(j)}, s^{*(j)}) = 1_{\mathbb{G}_T}$.
It outputs 0 otherwise.

[0104] ***実施の形態1の効果***

以上のように、実施の形態1に係る署名システム1は、ABPの述語ベクトルを用いてABE方式を実現する。これにより、実用的なABE方式が実現される。

[0105] 実施の形態1に係る署名システム1は、署名鍵SK (x) のインデックス部に係数としてインデックス情報I*を設定し、検証データのインデックス部に係数としてインデックス情報Iを設定する。インデックス情報I*の*ℓ*とインデックス情報Iの*ρ* (j) とが対応している場合には、署名sigの要素s* (j) と検証データの要素c (j) についてペアリング演算を行うと、インデックス部が0になる。インデックス情報I*の*ℓ*とインデックス情報Iの*ρ* (j) とが対応していない場合には、署名sigの要素s* (j) と検証データの要素c (j) についてペアリング演算を行っても、インデックス部が0にな

らない。

これにより、属性ベクトル $x \rightarrow$ の要素毎に別の基底を用いず、属性ベクトル $x \rightarrow$ の全ての要素に共通の基底 B_1 及び基底 B^*_1 を用いても、安全性を確保することが可能になる。その結果、属性ベクトル $x \rightarrow$ の要素数によらず、公開パラメータ MPK に基底 $B^{\wedge}_1$ 及び基底 $B^{\wedge,*}_1$ を含めておけばよい。つまり、公開パラメータ MPK を変更することなく、使用する属性ベクトル $x \rightarrow$ の要素数を任意に変更可能である。

[0106] ***他の構成***

＜変形例1＞

実施の形態1では、インデックス部として2次元分の基底ベクトルが用いられた。しかし、インデックス情報 l^* とインデックス情報 l との内積の和が0になるのであれば、インデックス部は何次元分の基底ベクトルが用いられてもよい。

[0107] ＜変形例2＞

実施の形態1では、各機能構成要素がソフトウェアで実現された。しかし、変形例2として、各機能構成要素はハードウェアで実現されてもよい。この変形例2について、実施の形態1と異なる点を説明する。

[0108] 図10を参照して、変形例2に係るセットアップ装置10の構成を説明する。

各機能構成要素がハードウェアで実現される場合には、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とに代えて、電子回路15を備える。電子回路15は、各機能構成要素と、メモリ12と、ストレージ13との機能とを実現する専用の回路である。

[0109] 図11を参照して、変形例2に係る鍵生成装置20の構成を説明する。

各機能構成要素がハードウェアで実現される場合には、鍵生成装置20は、プロセッサ21とメモリ22とストレージ23とに代えて、電子回路25を備える。電子回路25は、各機能構成要素と、メモリ22と、ストレージ23との機能とを実現する専用の回路である。

[0110] 図 1 2 を参照して、変形例 2 に係る署名装置 3 0 の構成を説明する。

各機能構成要素がハードウェアで実現される場合には、署名装置 3 0 は、プロセッサ 3 1 とメモリ 3 2 とストレージ 3 3 とに代えて、電子回路 3 5 を備える。電子回路 3 5 は、各機能構成要素と、メモリ 3 2 と、ストレージ 3 3 との機能とを実現する専用の回路である。

[0111] 図 1 3 を参照して、変形例 2 に係る検証装置 4 0 の構成を説明する。

各機能構成要素がハードウェアで実現される場合には、検証装置 4 0 は、プロセッサ 4 1 とメモリ 4 2 とストレージ 4 3 とに代えて、電子回路 4 5 を備える。電子回路 4 5 は、各機能構成要素と、メモリ 4 2 と、ストレージ 4 3 との機能とを実現する専用の回路である。

[0112] 電子回路 1 5, 2 5, 3 5, 4 5 としては、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ロジック IC、GA (Gate Array)、ASIC (Application Specific Integrated Circuit)、FPGA (Field-Programmable Gate Array) が想定される。

各機能構成要素を 1 つの電子回路 1 5, 2 5, 3 5, 4 5 で実現してもよいし、各機能構成要素を複数の電子回路 1 5, 2 5, 3 5, 4 5 に分散させて実現してもよい。

[0113] <変形例 3>

変形例 3 として、一部の各機能構成要素がハードウェアで実現され、他の各機能構成要素がソフトウェアで実現されてもよい。

[0114] プロセッサ 1 1, 2 1, 3 1, 4 1 とメモリ 1 2, 2 2, 3 2, 4 2 とストレージ 1 3, 2 3, 3 3, 4 3 と電子回路 1 5, 2 5, 3 5, 4 5 とを処理回路という。つまり、各機能構成要素の機能は、処理回路により実現される。

符号の説明

[0115] 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

レンジ、１４

通信インタフェース、１５ 電子回路、１１１ 受付部、１１２ マスター鍵生成部、１１３ 出力部、２０ 鍵生成装置、２１ プロセッサ、２２ メモリ、２３ ストレージ、２４ 通信インタフェース、２５ 電子回路、２１１ 取得部、２１２ 署名鍵生成部、２１３ 出力部、３０ 署名装置、３１ プロセッサ、３２ メモリ、３３ ストレージ、３４ 通信インタフェース、３５ 電子回路、３１１ 取得部、３１２ 署名部、３１３ 出力部、４０ 検証装置、４１ プロセッサ、４２ メモリ、４３ ストレージ、４４ 通信インタフェース、４５ 電子回路、１ 署名システム。

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、属性ベクトルが設定された署名鍵を取得する取得部と、
- 前記取得部によって取得された前記署名鍵に対して、 ABP (Arithmetic Branching Programs) の述語情報を設定して、メッセージに対する署名を生成する署名部と、
- 前記署名部によって生成された前記署名と、前記メッセージとを出力する出力部と
- を備える署名装置。
- [請求項2] 前記署名鍵は、前記属性ベクトルの要素毎に対応する要素を含み、前記署名鍵の要素は、前記基底 B^* における一部の基底ベクトルの係数として、前記属性ベクトルの対応する要素に応じたインデックス情報 l^* が設定された
- 請求項 1 に記載の署名装置。
- [請求項3] 前記述語情報は、前記 ABP に対応する ASP (Arithmetic Span Programs) 表現から得られた
- 請求項 1 又は 2 に記載の署名装置。
- [請求項4] 前記述語情報は、数 1 に示す要素 Ω_j を含み、
- 前記署名部は、前記要素 Ω_j により前記属性ベクトルの要素を隠蔽する
- 請求項 3 に記載の署名装置。

[数1]

$$\vec{e}(L,L) = \sum_{j \in [m]} \Omega_j(x_{\rho(j)} \vec{y}^{(j)} + \vec{z}^{(j)})$$

ここで、

$$\vec{e}(d,i) = (\overbrace{0,\dots,0}^{i-1}, \overbrace{1,0,\dots,0}^{d-i}) \text{ for } i \in [d],$$

d は 1 以上の整数、

$\mathcal{S}$ は A S P 表現されたアクセスストラクチャであり、

$$\mathcal{S} = (\mathcal{U} = \{\vec{y}^{(j)}, \vec{z}^{(j)}\}_{j \in [m]} \subset (\mathbb{F}_q^L)^2, \rho: [m] \rightarrow [n]),$$

n は属性ベクトルの要素数、

m, L は 1 以上の整数

[請求項5]

前記述語情報は、数 2 に示す要素 Ω'_j 及び要素 Ω''_j を含み、

前記署名部は、前記要素 Ω'_j 及び前記要素 Ω''_j により前記属性ベクトルの要素と前記要素 Ω_j とを隠蔽する

請求項 4 に記載の署名装置。

[数2]

$$((\Omega'_j)_{j \in [m]}, (\Omega''_j)_{j \in [m]}) \xleftarrow{U} (\mathbb{F}_q^m)^2$$

$$\text{such that } \sum_{j \in [m]} (\Omega'_j \vec{y}^{(j)} + \Omega''_j \vec{z}^{(j)}) = \vec{0}^L$$

[請求項6]

前記署名は、数 3 に示す s i g である

請求項 5 に記載の署名装置。

[数3]

$$sig = (s^{*(0)}, \dots, s^{*(m+1)})$$

ここで、

$$s^{*(0)} = \xi k^{*(0)} + r^{*(0)},$$

$$s^{*(j)} = \xi \Omega_j k^{*(\rho(j))} + \sigma'_j (b^{*(1,1)} + \rho(j) b^{*(1,2)}) \\ + \Omega''_j b^{*(1,3)} + \Omega'_j b^{*(1,4)} + r^{*(j)} \text{ for } j \in [m],$$

$$s^{*(m+1)} = \xi (k^{*(n+1,1)} + H(MSG \| S) k^{*(n+1,2)}) + r^{*(m+1)},$$

$$\xi, \sigma'_j \xleftarrow{U} \mathbb{F}_q,$$

$$r^{*(0)} \xleftarrow{U} \text{SPAN} \langle b^{*(0,3)} \rangle, r^{*(j)} \xleftarrow{U} \text{SPAN} \langle b^{*(1,1)}, b^{*(1,2)} \rangle,$$

$$r^{*(m+1)} \xleftarrow{U} \text{SPAN} \langle b^{*(2,5)}, b^{*(2,6)} \rangle,$$

$k^{*(0)}, \dots, k^{*(n)}, k^{*(n+1,1)}, k^{*(n+1,2)}$ は署名鍵の要素であり、

$$k^{*(0)} = (\omega, 0, \phi_0, 0)_{\mathbb{B}_0},$$

$$k^{*(\iota)} = (\sigma_\iota(1, \iota), \omega(1, x_\iota), \vec{0}^6, \vec{\phi}(\iota), \vec{0}^2)_{\mathbb{B}_1},$$

$$k^{*(n+1,1)} = (\omega(1, 0), \vec{0}^2, \vec{\phi}^{(n+1,1)}, \vec{0}^2)_{\mathbb{B}_2} \text{ for } \iota \in [n],$$

$$k^{*(n+1,2)} = (\omega(1, 0), \vec{0}^2, \vec{\phi}^{(n+1,2)}, \vec{0}^2)_{\mathbb{B}_2},$$

$$\omega \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \phi_0 \xleftarrow{U} \mathbb{F}_q,$$

$$\text{for } \iota \in [n] \sigma_\iota \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \vec{\phi}(\iota), \vec{\phi}^{(n+1,1)}, \vec{\phi}^{(n+1,2)} \xleftarrow{U} \mathbb{F}_q^2,$$

H はハッシュ関数、 MSG はメッセージ、 b^* は基底 B^* の基底ベクトル

[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) の述語情報とが設定された署名を取得する取得部と、

前記取得部によって取得された前記署名と、前記基底 B に検証情報を設定した検証データとについてペアリング演算を行うことにより、前記署名を検証する検証部とを備える検証装置。

[請求項8] 前記署名は、前記属性ベクトルの要素毎に対応する要素を含み、前記署名の要素は、前記基底 B^* における一部の基底ベクトルの係数として、前記属性ベクトルにおける対応する要素に応じたインデックス情報 I^* が設定され、

前記検証データは、前記属性ベクトルの1つ以上の要素に対応する要素を含み、前記検証データの要素は、前記一部の基底ベクトルに対応する前記基底 B における基底ベクトルの係数として、前記インデックス情報 I^* との内積の和が0になるインデックス情報 I が設定された

請求項7に記載の検証装置。

[請求項9] 前記述語情報及び前記検証情報は、前記 ABP に対応する ASP (Arithmetic Span Programs) 表現から得られた

請求項7又は8に記載の検証装置。

[請求項10] 述語情報は、数4に示す Ω_j を含む

請求項9に記載の検証装置。

[数4]

$$\vec{e}^{(L,L)} = \sum_{j \in [m]} \Omega_j(x_{\rho(j)} \vec{y}^{(j)} + \vec{z}^{(j)})$$

ここで、

$$\vec{e}^{(d,i)} = (\overbrace{0, \dots, 0}^{i-1}, \overbrace{1, 0, \dots, 0}^{d-i}) \text{ for } i \in [d],$$

d は1以上の整数、

$\mathcal{S}$ は ASP 表現されたアクセスストラクチャであり、

$$\mathcal{S} = (U = \{\vec{y}^{(j)}, \vec{z}^{(j)}\}_{j \in [m]} \subset (\mathbb{F}_q^L)^2, \rho: [m] \rightarrow [n]),$$

n は属性ベクトルの要素数、

m, L は1以上の整数

[請求項11] 前記署名は、数5に示す sig であり、

前記検証データは、数6に示す c である

請求項 10 に記載の検証装置。

[数5]

$$sig = (s^{*(0)}, \dots, s^{*(m+1)})$$

ここで、

$$s^{*(0)} = \xi k^{*(0)} + r^{*(0)},$$

$$s^{*(j)} = \xi \Omega_j k^{*(\rho(j))} + \sigma'_j (b^{*(1,1)} + \rho(j) b^{*(1,2)}) \\ + \Omega''_j b^{*(1,3)} + \Omega'_j b^{*(1,4)} + r^{*(j)} \text{ for } j \in [m],$$

$$s^{*(m+1)} = \xi (k^{*(n+1,1)} + H(MSG \| S) k^{*(n+1,2)}) + r^{*(m+1)},$$

$$\xi, \sigma'_j \xleftarrow{U} \mathbb{F}_q,$$

$$r^{*(0)} \xleftarrow{U} \text{SPAN} \langle b^{*(0,3)} \rangle, r^{*(j)} \xleftarrow{U} \text{SPAN} \langle b^{*(1,1)}, b^{*(1,2)} \rangle,$$

$$r^{*(m+1)} \xleftarrow{U} \text{SPAN} \langle b^{*(2,5)}, b^{*(2,6)} \rangle,$$

$$((\Omega'_j)_{j \in [m]}, (\Omega''_j)_{j \in [m]}) \xleftarrow{U} (\mathbb{F}_q^m)^2$$

$$\text{such that } \sum_{j \in [m]} (\Omega'_j \bar{y}^{(j)} + \Omega''_j \bar{z}^{(j)}) = \bar{0}L,$$

$k^{*(0)}, \dots, k^{*(n)}, k^{*(n+1,1)}, k^{*(n+1,2)}$ は署名鍵の要素であり、

$$k^{*(0)} = (\omega, 0, \phi_0, 0)_{\mathbb{B}_0^*},$$

$$k^{*(\iota)} = (\sigma_\iota(1, \iota), \omega(1, x_\iota), \bar{0}^6, \bar{\phi}^{(\iota)}, \bar{0}^2)_{\mathbb{B}_1^*},$$

$$k^{*(n+1,1)} = (\omega(1, 0), \bar{0}^2, \bar{\phi}^{(n+1,1)}, \bar{0}^2)_{\mathbb{B}_2^*} \text{ for } \iota \in [n],$$

$$k^{*(n+1,2)} = (\omega(1, 0), \bar{0}^2, \bar{\phi}^{(n+1,2)}, \bar{0}^2)_{\mathbb{B}_2^*},$$

$$\omega \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \phi_0 \xleftarrow{U} \mathbb{F}_q,$$

$$\text{for } \iota \in [n] \sigma_\iota \xleftarrow{U} \mathbb{F}_q \setminus \{0\}, \bar{\phi}^{(\iota)}, \bar{\phi}^{(n+1,1)}, \bar{\phi}^{(n+1,2)} \xleftarrow{U} \mathbb{F}_q^2,$$

H はハッシュ関数、 MSG はメッセージ、 b^* は基底 B^* の基底ベクトル

[数6]

$$c = (c^{(0)}, \dots, c^{(m+1)})$$

ここで、

$$c^{(0)} = (-u - u_L, 0, 0, \eta_0)_{\mathbb{B}_0}$$

$$c^{(j)} = (\mu_j(\rho(j), -1), (s'_j, s_j), \vec{0}^6, \vec{0}^2, \vec{\eta}^{(j)})_{\mathbb{B}_1} \text{ for } j \in [m]$$

$$c^{(m+1)} = ((u - \kappa H(MSG \| S), \kappa), \vec{0}^2, \vec{0}^2, \vec{\eta}^{(m+1)})_{\mathbb{B}_2}$$

$$\vec{u} = (u_1, \dots, u_L) \xleftarrow{U} \mathbb{F}_q^L,$$

$$\text{for } j \in [m] \ s_j = \vec{u} \cdot \vec{y}^{(j)}, \ s'_j = \vec{u} \cdot \vec{z}^{(j)},$$

$$u, \eta_0, \kappa \xleftarrow{U} \mathbb{F}_q, \ \mu_j \xleftarrow{U} \mathbb{F}_q \text{ for } j \in [m],$$

$$\vec{\eta}^{(j)}, \vec{\eta}^{(m+1)} \xleftarrow{U} \mathbb{F}_q^2$$

[請求項12]

署名装置における取得部が、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、属性ベクトルが設定された署名鍵を取得し、

前記署名装置における署名部が、前記署名鍵に対して、ABP (Arithmetic

Branching Programs)の述語情報を設定して、メッセージに対する署名を生成し、

前記署名装置における出力部が、前記署名と、前記メッセージとを出力する署名方法。

[請求項13]

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、属性ベクトルが設定された署名鍵を取得する取得処理と、

前記取得処理によって取得された前記署名鍵に対して、ABP (Arithmetic

Branching Programs)の述語情報を設定して、メッセージに対する署名を生成する署名処理と、

前記署名処理によって生成された前記署名と、前記メッセージとを

出力する出力処理とを行う署名装置としてコンピュータを機能させる署名プログラム。

[請求項14] 検証装置における取得部が、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) の述語情報とが設定された署名を取得し、

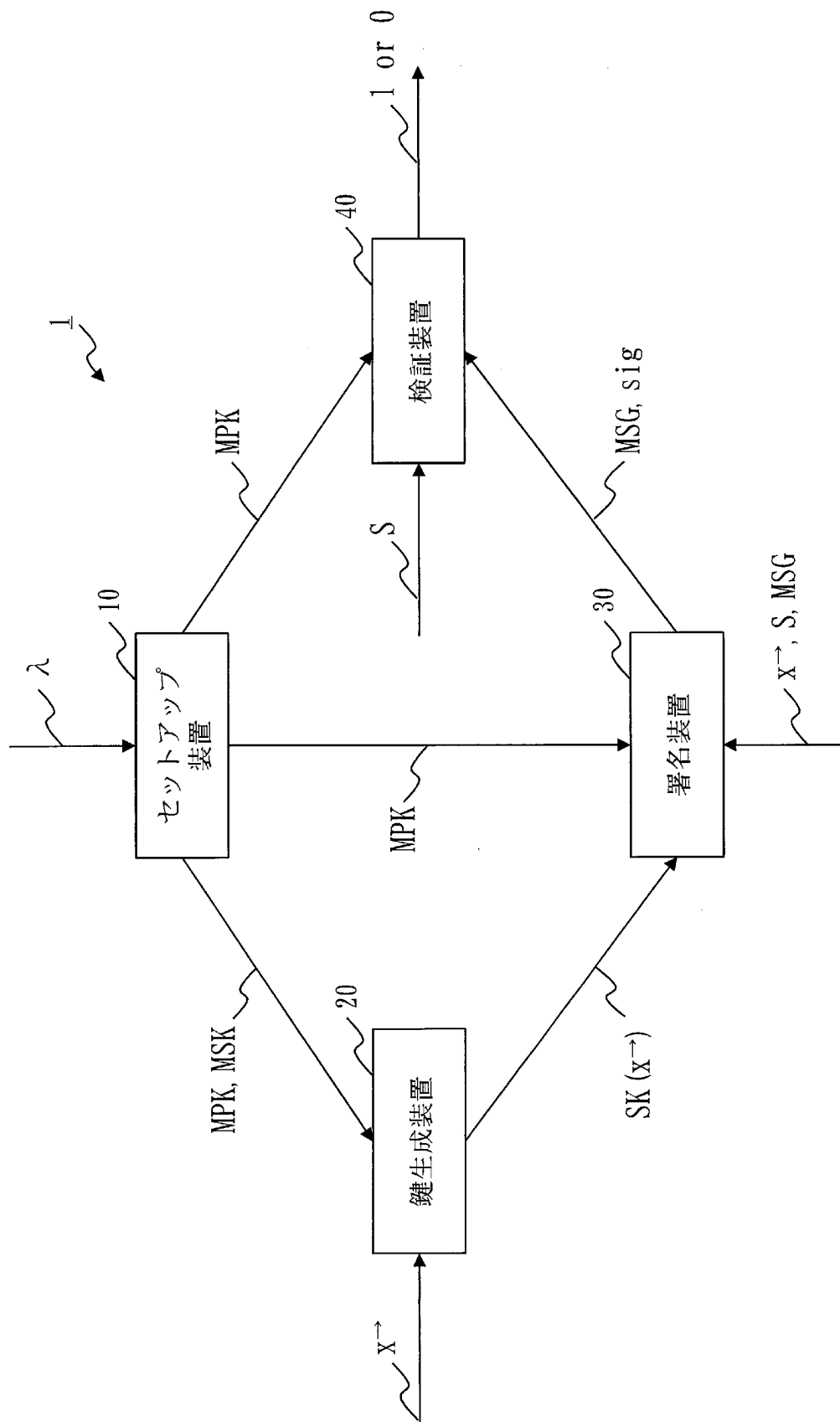
前記検証装置における検証部が、前記署名と、前記基底Bに検証情報を設定した検証データとについてペアリング演算を行うことにより、前記署名を検証する検証方法。

[請求項15] 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) の述語情報とが設定された署名を取得する取得処理と、

前記取得処理によって取得された前記署名と、前記基底Bに検証情報を設定した検証データとについてペアリング演算を行うことにより、前記署名を検証する検証処理と
を行う検証装置としてコンピュータを機能させる検証プログラム。

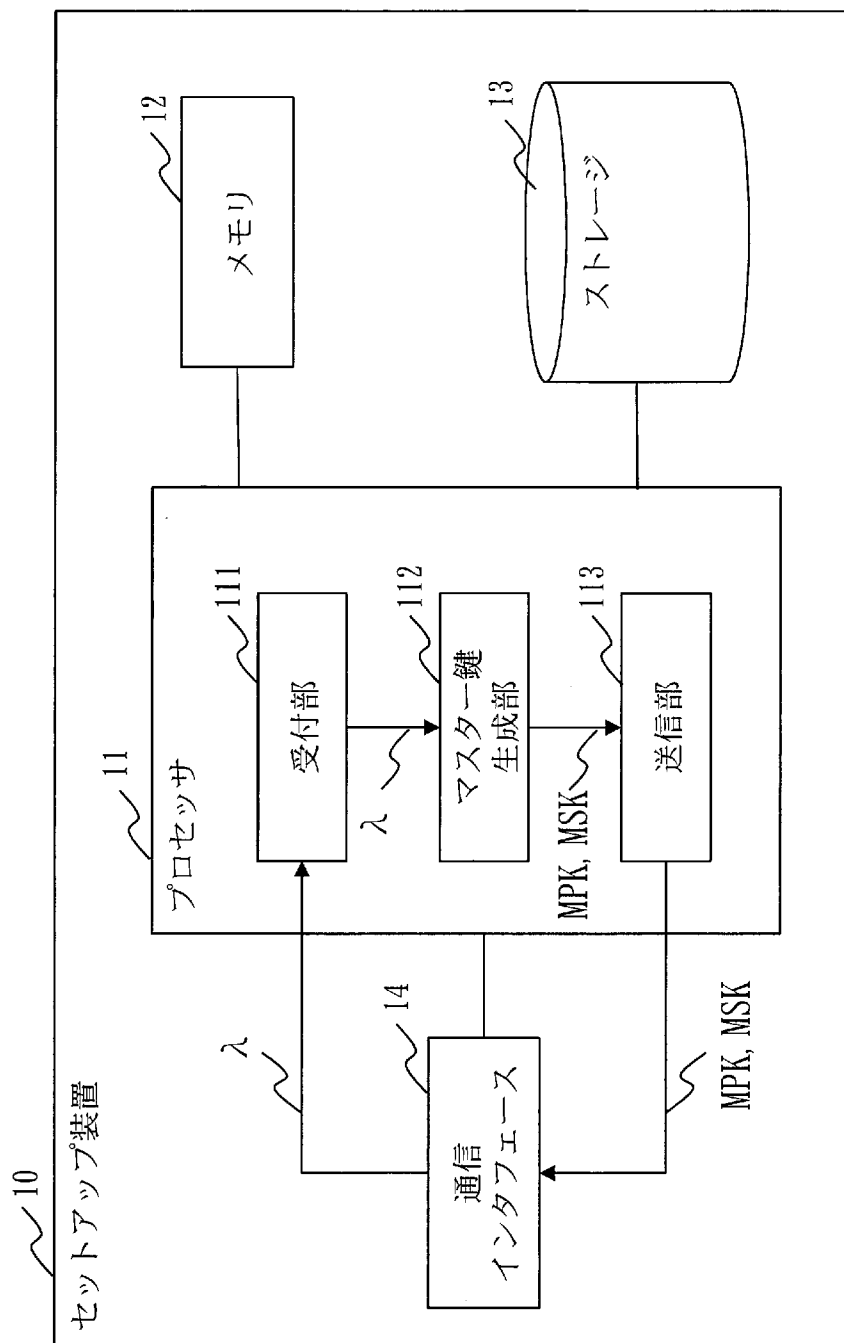
[図1]

図1



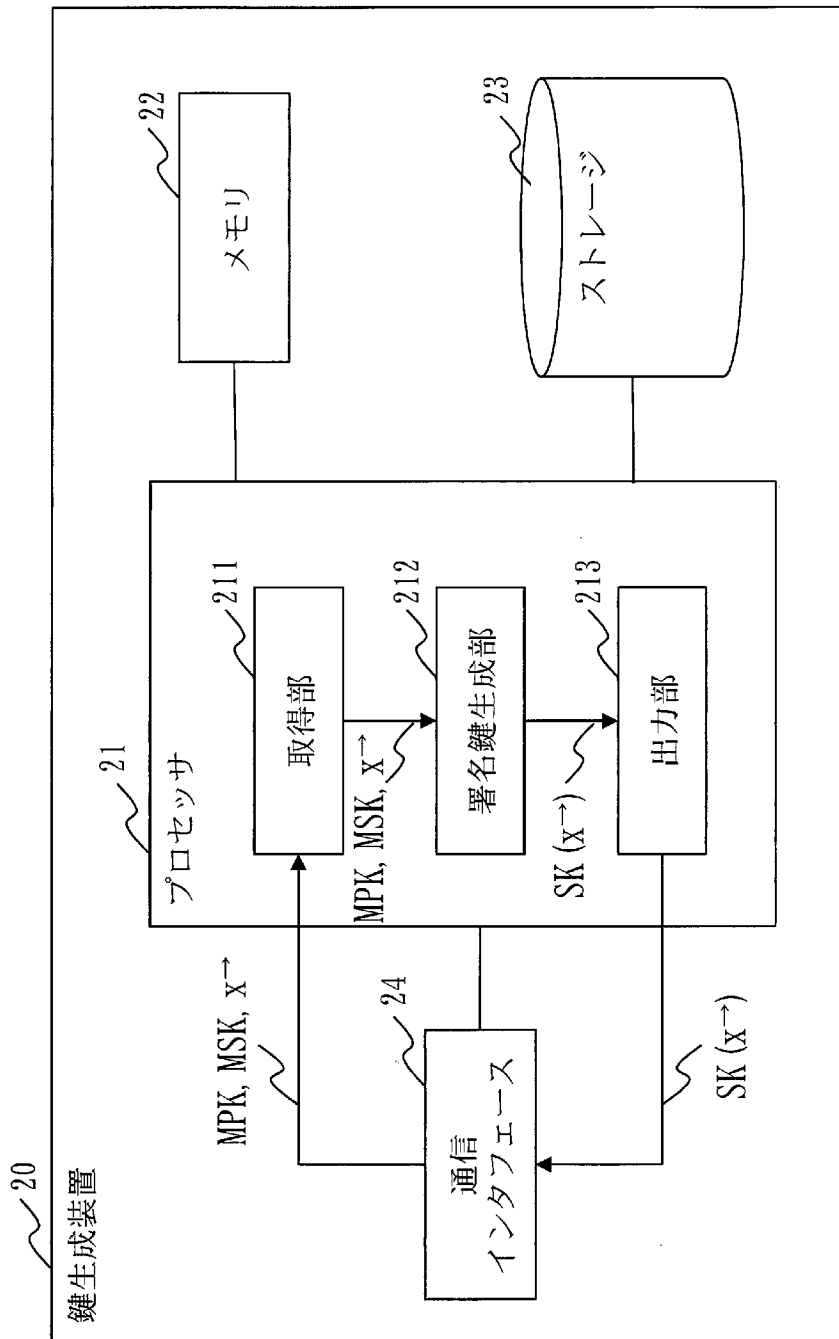
[図2]

図2



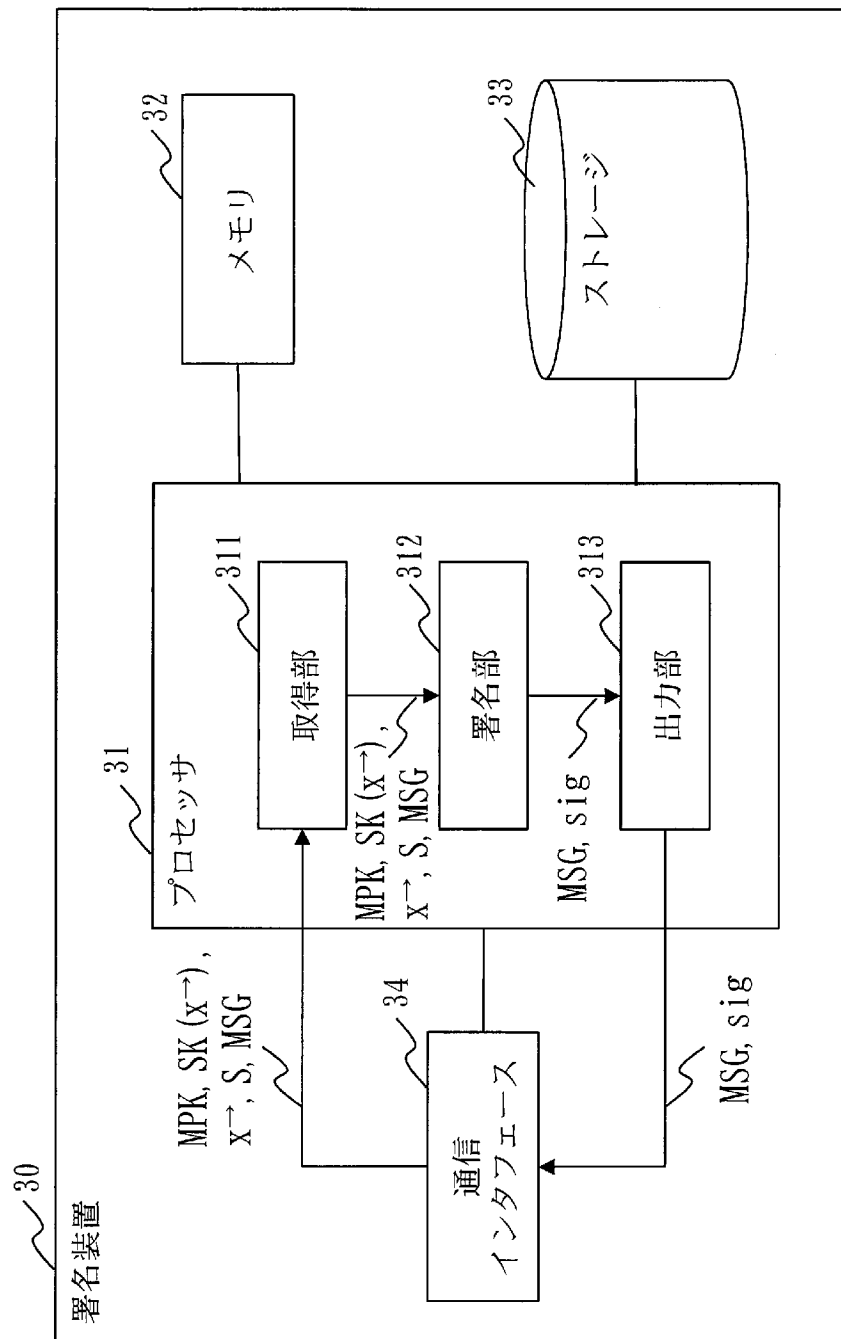
[図3]

図3



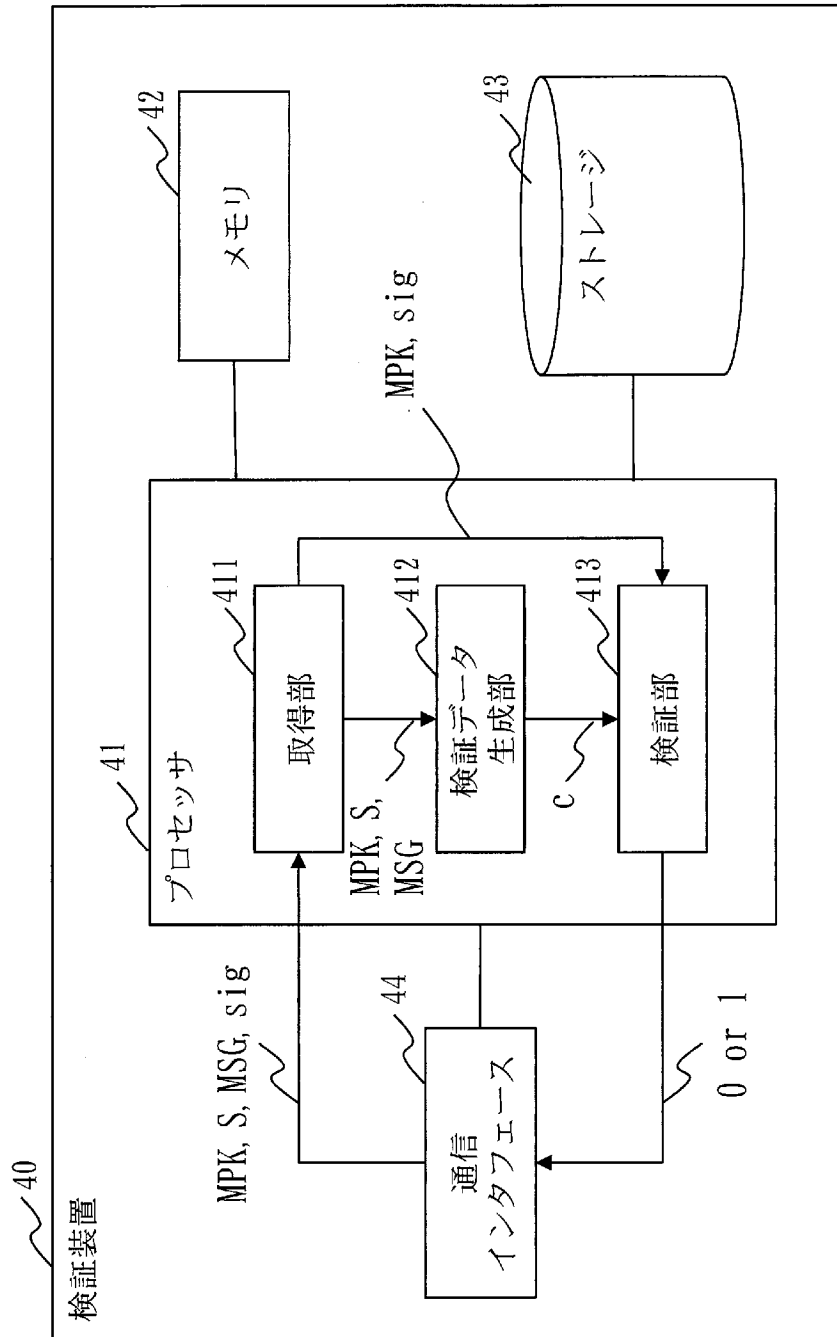
[図4]

図4



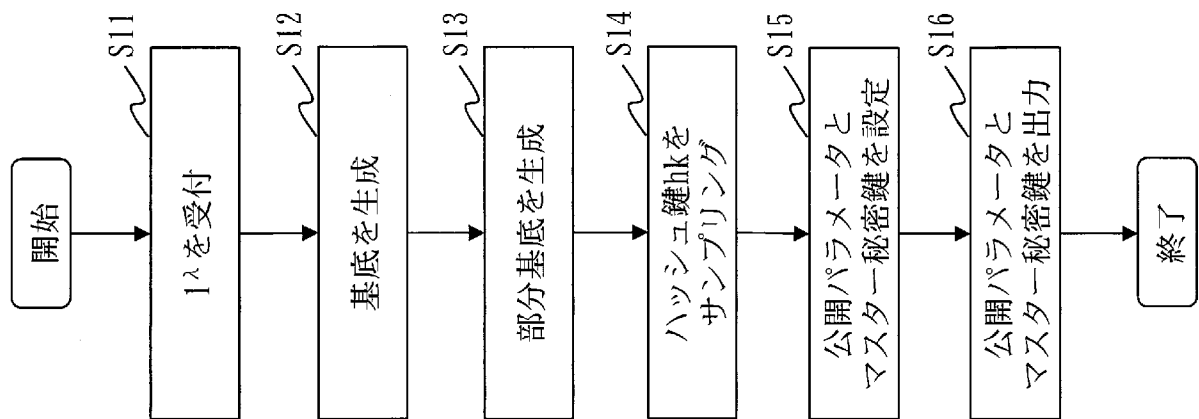
[図5]

図5



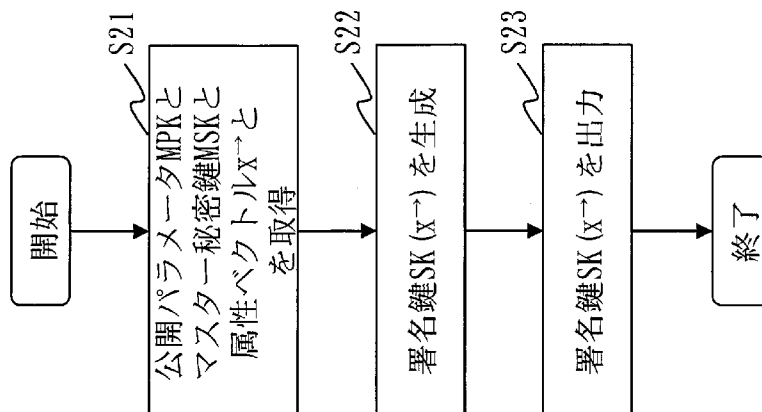
[図6]

図6



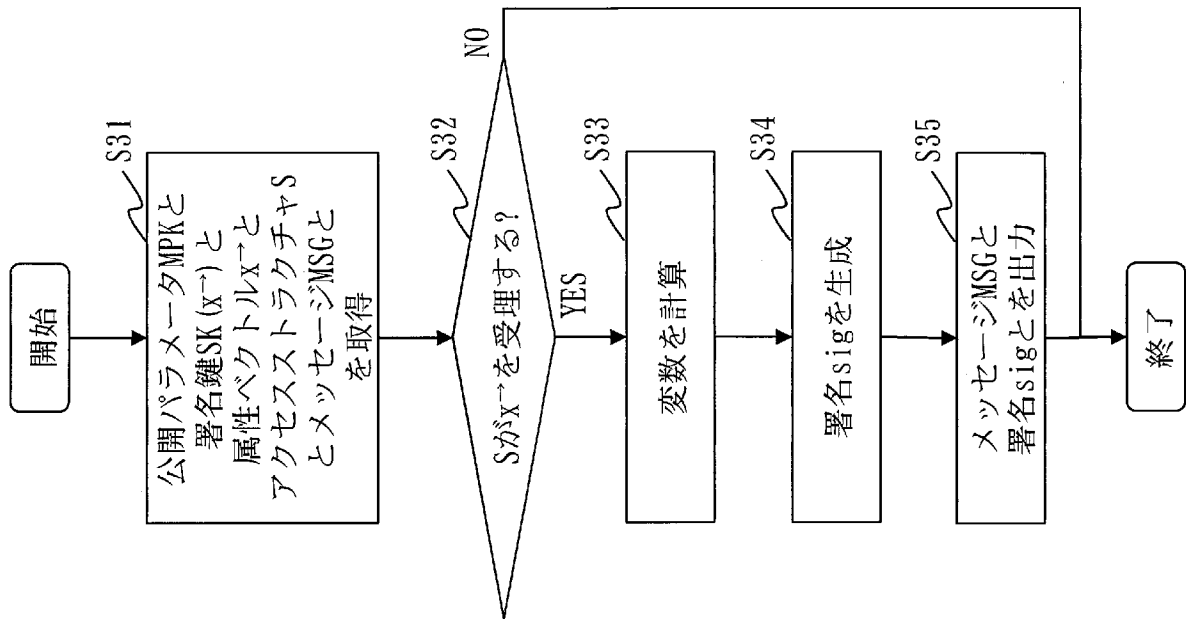
[図7]

図7



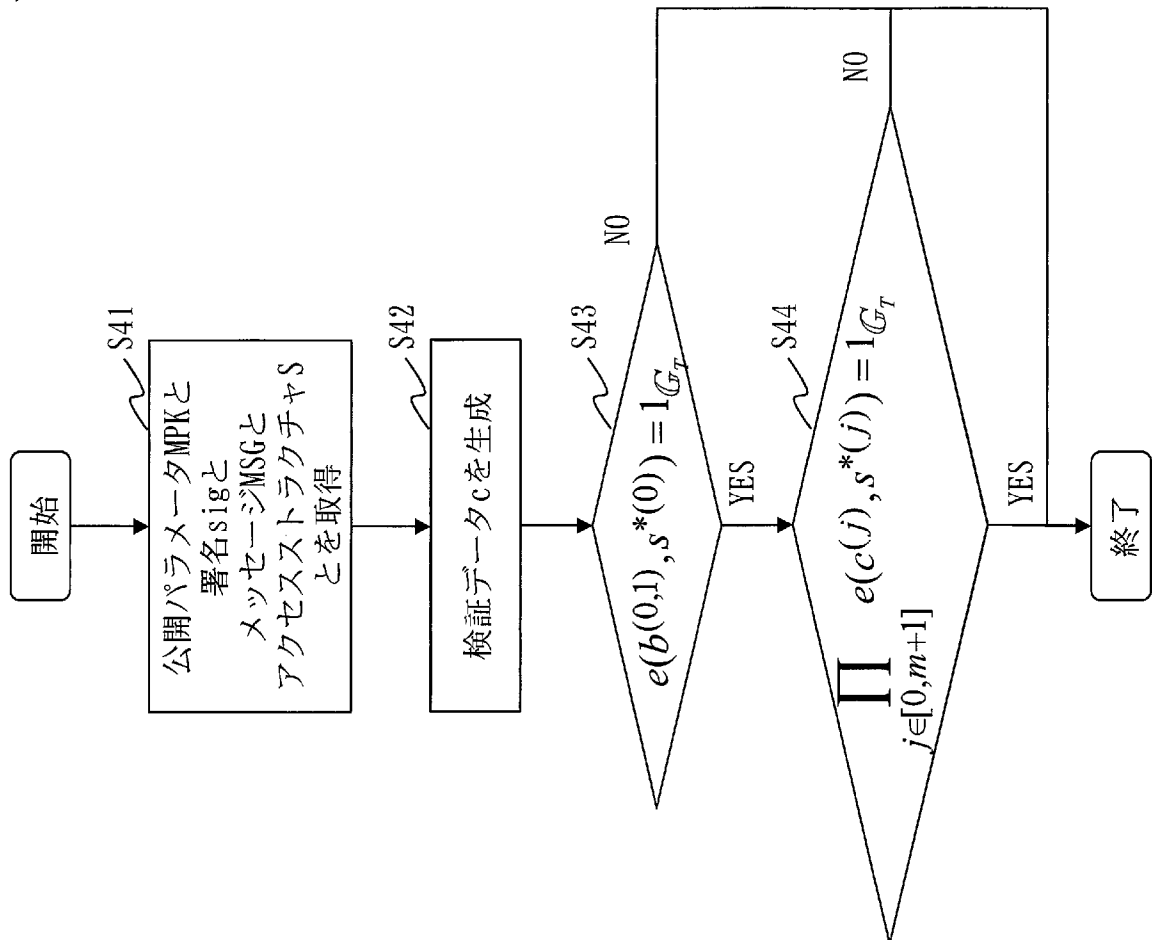
[図8]

図8



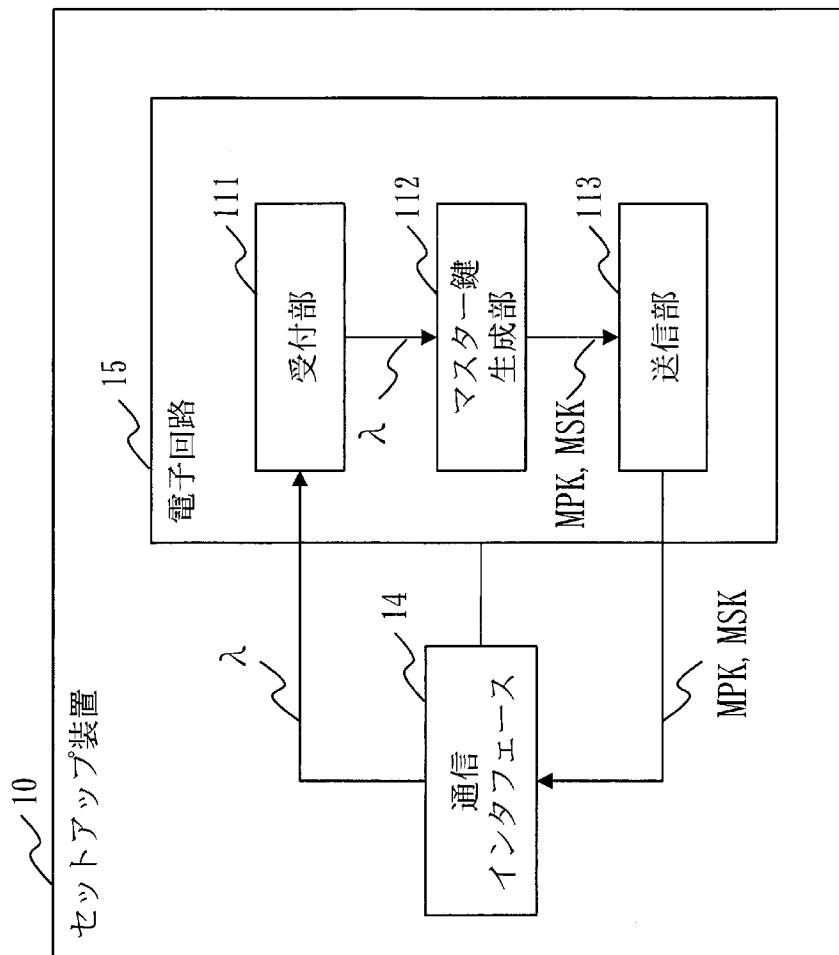
[図9]

図9



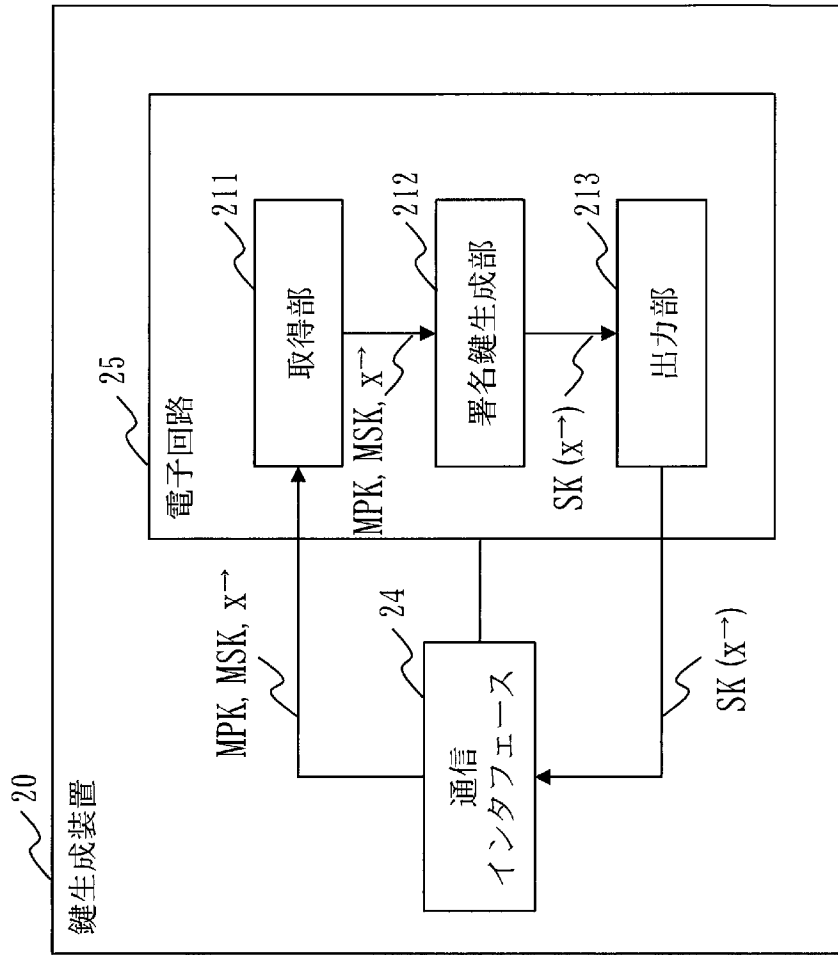
[図10]

図10



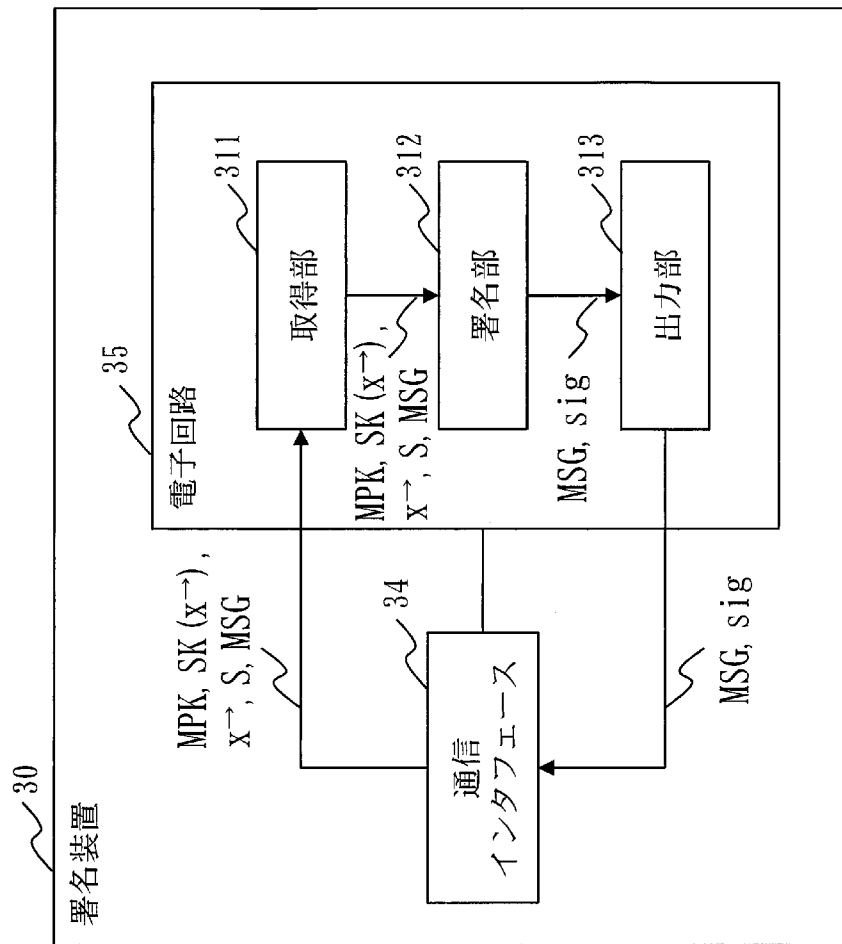
[図11]

図11



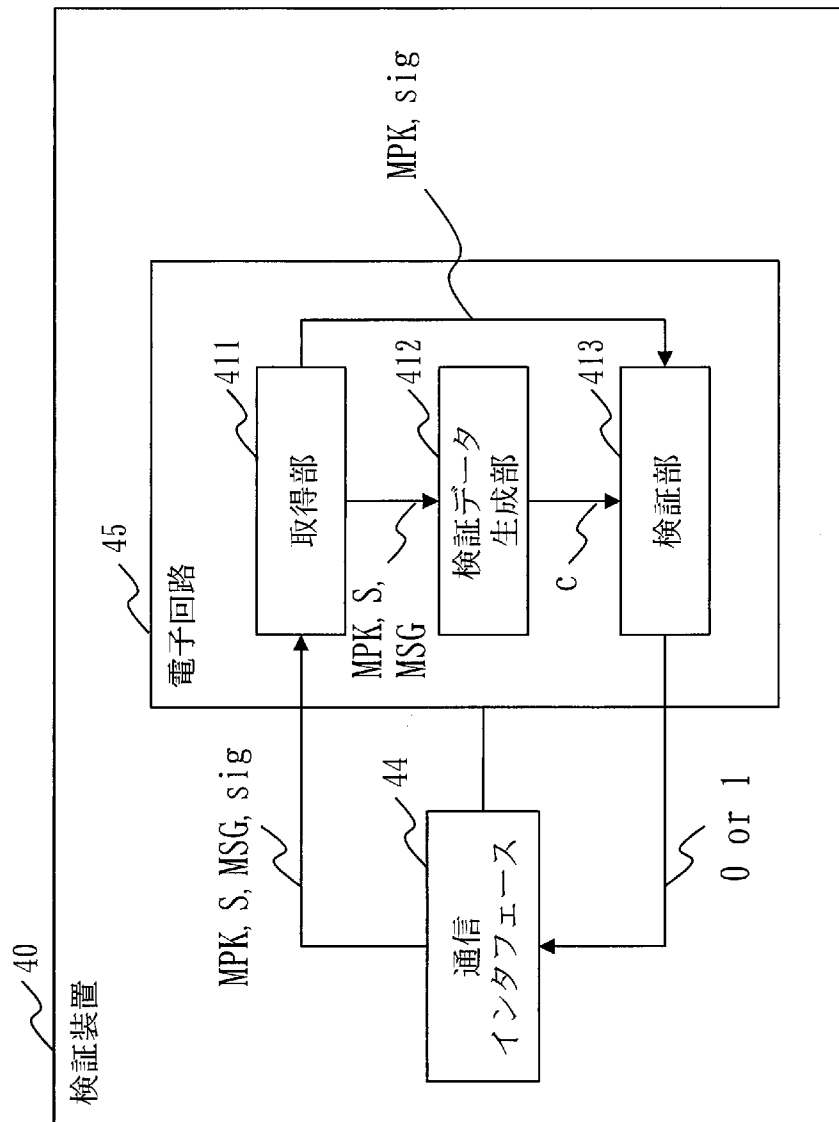
[図12]

図12



[図13]

図13



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/047995

A. CLASSIFICATION OF SUBJECT MATTER

G09C 1/00 (2006.01)i; H04L 9/14 (2006.01)i; H04L 9/32 (2006.01)i
FI: H04L9/00 675B; H04L9/00 641; G09C1/00 640D

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G09C1/00; H04L9/14; H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-155088 A (MITSUBISHI ELECTRIC CORP.) 16.08.2012 (2012-08-16) paragraphs [0045]-[0095], [0154]-[0158], fig. 5-13, 23	1-15
A	WO 2012/108100 A1 (MITSUBISHI ELECTRIC CORP.) 16.08.2012 (2012-08-16) paragraphs [0024]-[0026], fig. 6	1-15
A	US 2017/0351867 A1 (GIESECKE & DEVRIENT GMBH) 07.12.2017 (2017-12-07) paragraph [0027], fig. 2	1-15
A	DATTA, Pratishi et al., "Adaptively Simulation-Secure Attribute-Hiding Predicate Encryption", Cryptology ePrint Archive: Report 2018/1093, [retrieval date 04 February 2020], [online], 13 November 2018, version: 20181113:005554, internet:<URL:https://eprint.iacr.org/2018/1093.pdf>, abstract	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
06 February 2020 (06.02.2020)

Date of mailing of the international search report
18 February 2020 (18.02.2020)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2019/047995

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2012-155088 A	16 Aug. 2012	US 2013/0322627 A1 paragraphs [0210]- [0364], fig. 5-13, 23 WO 2012/101913 A1 EP 2670081 A1 CN 103348624 A KR 10-2013-0130810 A	
WO 2012/108100 A1	16 Aug. 2012	US 2013/0336474 A1 paragraphs [0122]- [0134], fig. 6 EP 2675107 A1 CN 103354984 A KR 10-2013-0122678 A	
US 2017/0351867 A1	07 Dec. 2017	WO 2016/096117 A1 EP 3234853 A1 DE 102014018889 A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G09C 1/00(2006.01)i; H04L 9/14(2006.01)i; H04L 9/32(2006.01)i FI: H04L9/00 675B; H04L9/00 641; G09C1/00 640D										
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（IPC）） G09C1/00; H04L9/14; H04L9/32 最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2020年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2020年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2020年</td> </tr> </table> 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）			日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2020年	日本国実用新案登録公報	1996-2020年	日本国登録実用新案公報	1994-2020年
日本国実用新案公報	1922-1996年									
日本国公開実用新案公報	1971-2020年									
日本国実用新案登録公報	1996-2020年									
日本国登録実用新案公報	1994-2020年									
C. 関連すると認められる文献										
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号								
A	JP 2012-155088 A（三菱電機株式会社）16.08.2012（2012-08-16） 段落 [0045] - [0095]、[0154] - [0158]、図5-13、 23	1-15								
A	WO 2012/108100 A1（三菱電機株式会社）16.08.2012（2012-08-16） 段落 [0024] - [0026]、図6	1-15								
A	US 2017/0351867 A1（GIESECKE & DEVRIENT GMBH）07.12.2017（2017-12-07） 段落 [0027]、Fig. 2	1-15								
A	DATTA, Pratishi et al., Adaptively Simulation-Secure Attribute-Hiding Predicate Encryption, Cryptology ePrint Archive: Report 2018/1093, [検索日 2020.02.04], [オンライン], 2018.11.13, Version: 20181113:005554, インター ネット: <URL: https://eprint.iacr.org/2018/1093.pdf> Abstract	1-15								
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。										
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に 公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若し くは他の特別な理由を確立するために引用する文献（理由を 付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の 後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵 触するものではなく、発明の原理又は理論の理解のために引 用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性 又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献 との、当業者にとって自明である組合せによって進歩性がな いと考えられるもの “&” 同一パテントファミリー文献										
国際調査を完了した日 06.02.2020		国際調査報告の発送日 18.02.2020								
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 青木 重徳 5S 4229 電話番号 03-3581-1101 内線 3546								

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2019/047995

引用文献			公表日	パテントファミリー文献	公表日
JP	2012-155088	A	16.08.2012	US 2013/0322627 A1 段落[0210]-[0364], Figs. 5-13, 23 WO 2012/101913 A1 EP 2670081 A1 CN 103348624 A KR 10-2013-0130810 A	
WO	2012/108100	A1	16.08.2012	US 2013/0336474 A1 段落[0122]-[0134], Fig. 6 EP 2675107 A1 CN 103354984 A KR 10-2013-0122678 A	
US	2017/0351867	A1	07.12.2017	WO 2016/096117 A1 EP 3234853 A1 DE 102014018889 A	