(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
2014 年 2 月 6 日(06.02.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/021102 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2013/069368

(22) 国際出願日: 2013 年 7 月 17 日(17.07.2013)

(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 2012-170001 2012 年 7 月 31 日(31.07.2012) 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二丁目３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 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 溝井 章司, 外(MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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.

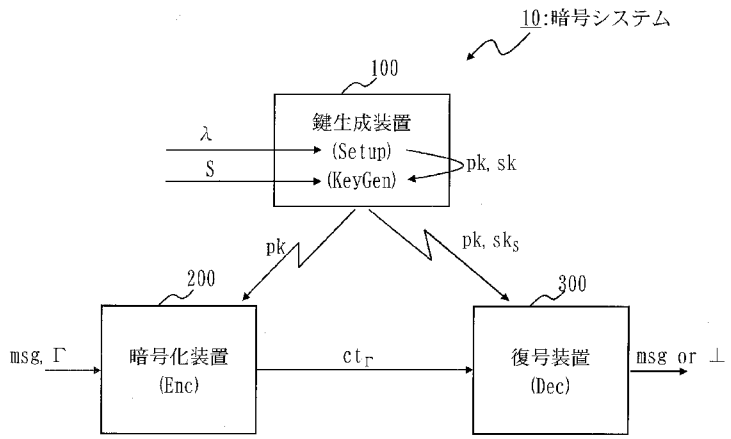
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: ENCRYPTION SYSTEM, ENCRYPTION METHOD, ENCRYPTION PROGRAM AND DECRYPTION DEVICE

(54) 発明の名称 : 暗号システム、暗号方法、暗号プログラム及び復号装置

[図3]



10 Encryption system
100 Key generation device
200 Encryption device
300 Decryption device

(57) **Abstract**: The purpose of the present invention is to broaden a range of what can be expressed by a relationship R in a function-type encryption method where, when decoding an encryption key ek in which a parameter Φ is set with a decryption key dk in which a parameter Ψ is set, the decryption key dk can decode a ciphertext encrypted with the encryption key ek only when the relationship R (Φ, Ψ) is satisfied. Of first information including a polynomial expression d(x), a plurality of polynomial expressions $D_i(x)$, and predicate information, and second information including attribute information, an encryption system (10) defines one as a ciphertext and defines the other as a decryption key. A decryption device (300) selects at least a part of the polynomial expressions $D_i(x)$ from among the plurality of polynomial expressions $D_i(x)$ on the basis of the predicate information and the attribute information, and calculates a coefficient Δ_i which makes it possible to divide a polynomial expression constituted on the basis of the polynomial expression $\Delta_i D_i(x)$ that is the selected polynomial expression $D_i(x)$ multiplied by the coefficient Δ_i, by the polynomial expression d(x). The decryption device (300) decodes the ciphertext on the basis of the calculated coefficient Δ_i.

(57) 要約:

[続葉有]

WO 2014/021102 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

パラメータΦが設定された暗号化鍵ｅｋをパラメータΨが設定された復号鍵ｄｋで復号する場合に、関係Ｒ（Φ，Ψ）が成立する場合に限り、復号鍵ｄｋは暗号化鍵ｅｋで暗号化された暗号文を復号することができる関数型暗号方式において、関係Ｒとして表現できる範囲を広くすることを目的とする。暗号システム１０は、多項式ｄ（ｘ）と複数の多項式D_i（ｘ）と述語情報とを含む第１情報と、属性情報を含む第２情報とのうちの一方を暗号文とし、他方を復号鍵とする。復号装置３００は、述語情報と属性情報とに基づき、複数の多項式D_i（ｘ）から少なくとも一部の多項式D_j（ｘ）を選択し、選択した多項式D_i（ｘ）に係数Δ_iを掛けた多項式$\Delta_i D_i$（ｘ）に基づき構成される多項式を、多項式ｄ（ｘ）で割り切れるようにする係数Δ_iを計算する。復号装置３００は、計算した係数Δ_iに基づき、前記暗号文を復号する。

明　細　書

発明の名称 ：

暗号システム、暗号方法、暗号プログラム及び復号装置

技術分野

[0001] この発明は、２次スパンプログラムの考えを利用した関数型暗号方式に関する。

背景技術

[0002] 関数型暗号方式は、暗号化鍵ｅｋと、復号鍵ｄｋとの間の関係をより高度化し、より柔軟にした暗号方式である。

関数型暗号方式において、暗号化鍵ｅｋと復号鍵ｄｋとには、それぞれ、パラメータΦとパラメータΨとが設定される。そして、関係Ｒ（Φ，Ψ）が成立する場合に限り、復号鍵ｄｋは暗号化鍵ｅｋで暗号化された暗号文を復号することができる。

[0003] 非特許文献３には、関数型暗号方式についての記載がある。

[0004] 非特許文献６には、２次スパンプログラムについての記載がある。

先行技術文献

非特許文献

[0005] 非特許文献1：Ｏｋａｍｏｔｏ，Ｔ．，Ｔａｋａｓｈｉｍａ，Ｋ．：Ｈｏｍｏｍｏｒｐｈｉｃ ｅｎｃｒｙｐｔｉｏｎ ａｎｄ ｓｉｇｎａｔｕｒｅｓ ｆｒｏｍ ｖｅｃｔｏｒ ｄｅｃｏｍｐｏｓｉｔｉｏｎ．Ｉｎ：Ｇａｌｂｒａｉｔｈ，Ｓ．Ｄ．，Ｐａｔｅｒｓｏｎ，Ｋ．Ｇ．（ｅｄｓ．）Ｐａｉｒｉｎｇ ２００８．ＬＮＣＳ，ｖｏｌ．５２０９，ｐｐ．５７－７４，Ｓｐｒｉｎｇｅｒ Ｈｅｉｄｅｌｂｅｒｇ（２００８）

非特許文献2：Ｏｋａｍｏｔｏ，Ｔ．，Ｔａｋａｓｈｉｍａ，Ｋ．：Ｈｉｅｒａｒｃｈｉｃａｌ ｐｒｅｄｉｃａｔｅ ｅｎｃｒｙｐｔｉｏｎ ｆｏｒ ｉｎｎｅｒ－ｐｒｏｄｕｃｔｓ，Ｉｎ：ＡＳＩＡＣＲＹＰＴ

２００９，Ｓｐｒｉｎｇｅｒ Ｈｅｉｄｅｌｂｅｒｇ（２００９）

非特許文献3：Ｏｋａｍｏｔｏ，Ｔ．，Ｔａｋａｓｈｉｍａ，Ｋ．：Ｆｕｌｌｙ ｓｅｃｕｒｅ ｆｕｎｃｔｉｏｎａｌ ｅｎｃｒｙｐｔｉｏｎ ｗｉｔｈ ｇｅｎｅｒａｌ ｒｅｌａｔｉｏｎｓ ｆｒｏｍ ｔｈｅ ｄｅｃｉｓｉｏｎａｌ ｌｉｎｅａｒ ａｓｓｕｍｐｔｉｏｎ．Ｉｎ：Ｒａｂｉｎ，Ｔ．（ｅｄ．）ＣＲＹＰＴＯ ２０１０．ＬＮＣＳ，ｖｏｌ．６２２３，ｐｐ．１９１－２０８．Ｓｐｒｉｎｇｅｒ Ｈｅｉｄｅｌｂｅｒｇ（２０１０）．Ｆｕｌｌ ｖｅｒｓｉｏｎ ｉｓ ａｖａｉｌａｂｌｅ ａｔ ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ／２０１０／５６３

非特許文献4：Ｏｋａｍｏｔｏ，Ｔ．，Ｔａｋａｓｈｉｍａ，Ｋ．：Ｅｆｆｉｃｉｅｎｔ ａｔｔｒｉｂｕｔｅ－ｂａｓｅｄ ｓｉｇｎａｔｕｒｅｓ ｆｏｒ ｎｏｎ－ｍｏｎｏｔｏｎｅ ｐｒｅｄｉｃａｔｅｓ ｉｎ ｔｈｅ ｓｔａｎｄａｒｄ ｍｏｄｅｌ，Ｉｎ：ＰＫＣ ２０１１，Ｓｐｒｉｎｇｅｒ Ｈｅｉｄｅｌｂｅｒｇ（２０１１）

非特許文献5：Ｏｋａｍｏｔｏ，Ｔ．，Ｔａｋａｓｈｉｍａ，Ｋ．：Ｄｅｃｅｎｔｒａｌｉｚｅｄ Ａｔｔｒｉｂｕｔｅ－Ｂａｓｅｄ Ｓｉｇｎａｔｕｒｅｓ ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ／２０１１／７０１

非特許文献6：Ｒｏｓａｒｉｏ Ｇｅｎｎａｒｏ ａｎｄ Ｃｒａｉｇ Ｇｅｎｔｒｙ ａｎｄ Ｂｒｙａｎ Ｐａｒｎｏ ａｎｄ Ｍａｒｉａｎａ Ｒａｙｋｏｖａ：Ｑｕａｄｒａｔｉｃ Ｓｐａｎ Ｐｒｏｇｒａｍｓ ａｎｄ Ｓｕｃｃｉｎｃｔ ＮＩＺＫｓ ｗｉｔｈｏｕｔ ＰＣＰｓ ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ／２０１２／２１５

発明の概要

発明が解決しようとする課題

[0006] 非特許文献３に記載された関数型暗号方式は、１次スパンプログラムを利用した方式である。この関数型暗号方式では、関係Ｒとして表現できる範囲

に限界がある。

この発明は、２次スパンプログラムの考えを利用することにより、関係Ｒとして表現できる範囲を広くすることが可能な関数型暗号方式を提供することを目的とする。

課題を解決するための手段

[0007] この発明に係る暗号システムは、

２次スパンプログラムを含む第１情報と、属性情報を含む第２情報とのうちの一方を暗号文として生成する暗号化装置と、

前記第１情報と前記第２情報とのうちの他方を復号鍵とし、前記２次スパンプログラムが前記属性情報を受理する場合に前記２次スパンプログラムと前記属性情報とから得られる情報に基づき、前記暗号文を復号する復号装置と

を備えることを特徴とする。

発明の効果

[0008] この発明に係る暗号システムでは、２次スパンプログラムの考えを利用することにより、関係Ｒとして表現できる範囲が理想化された範囲とすることが可能である。

図面の簡単な説明

[0009] [図1]２次スパンプログラムの説明図。

[図2]部分集合I_uの説明図。

[図3]ＫＰ－ＦＥ方式を実行する暗号システム１０の構成図。

[図4]ＣＰ－ＦＥ方式を実行する暗号システム１０の構成図。

[図5]実施の形態２に係る鍵生成装置１００の構成図。

[図6]実施の形態２に係る暗号化装置２００の構成図。

[図7]実施の形態２に係る復号装置３００の構成図。

[図8]実施の形態２に係るＳｅｔｕｐアルゴリズムの処理を示すフローチャート。

[図9]実施の形態２に係るＫｅｙＧｅｎアルゴリズムの処理を示すフローチャ

ート。

[図10]実施の形態２に係るＥｎｃアルゴリズムの処理を示すフローチャート。

[図11]実施の形態２に係るＤｅｃアルゴリズムの処理を示すフローチャート。

[図12]実施の形態４に係るＫｅｙＧｅｎアルゴリズムの処理を示すフローチャート。

[図13]鍵生成装置１００、暗号化装置２００、復号装置３００のハードウェア構成の一例を示す図。

発明を実施するための形態

[0010] 以下、図に基づき、発明の実施の形態を説明する。

以下の説明において、処理装置は後述するＣＰＵ９１１等である。記憶装置は後述するＲＯＭ９１３、ＲＡＭ９１４、磁気ディスク９２０等である。通信装置は後述する通信ボード９１５等である。入力装置は後述するキーボード９０２、通信ボード９１５等である。つまり、処理装置、記憶装置、通信装置、入力装置はハードウェアである。

[0011] 以下の説明における記法について説明する。

Ａがランダムな変数または分布であるとき、数１０１は、Ａの分布に従いＡからｙをランダムに選択することを表す。つまり、数１０１において、ｙは乱数である。

[数101]

$$y \xleftarrow{R} A$$

Ａが集合であるとき、数１０２は、Ａからｙを一様に選択することを表す。つまり、数１０２において、ｙは一様乱数である。

[数102]

$$y \xleftarrow{U} A$$

数１０３は、ｙがｚにより定義された集合であること、又はｙがｚを代入された集合であることを表す。

[数103]

$$y := z$$

ａが定数であるとき、数１０４は、機械（アルゴリズム）Ａが入力ｘに対しａを出力することを表す。

[数104]

$$A(x) \to a$$

例えば、

$$A(x) \to 1$$

数１０５、つまりＦ$_q$は、位数ｑの有限体を示す。

[数105]

$$\mathbb{F}_q$$

ベクトル表記は、有限体Ｆ$_q$におけるベクトル表示を表す。つまり、数１０６である。

[数106]

$\vec{x}$は、

$$(x_1,\ldots,x_n) \in \mathbb{F}_q^n$$

を示す。

数１０７は、数１０８に示す２つのベクトルｘ→とｖ→との数１０９に示す内積を表す。

[数107]

$$\vec{x} \cdot \vec{v}$$

[数108]

$$\vec{x} = (x_1, \ldots, x_n) ,$$

$$\vec{v} = (v_1, \ldots, v_n)$$

[数109]

$$\sum_{i=1}^{n} x_i v_i$$

X^Tは、行列Ｘの転置行列を表す。

b_i（ｉ＝１，．．．，ｎ）が空間Ｖのベクトルの要素であるとき、つまり、数１１０であるとき、数１１１は、数１１２によって生成される部分空間を表す。

[数110]

$$b_i \in \mathbb{V} \ (i = 1, \ldots, n)$$

[数111]

$$\mathrm{span}\langle b_1, \ldots, b_n \rangle \subseteq \mathbb{V} \ (\mathrm{resp.}\ \mathrm{span}\langle \vec{x}_1, \ldots, \vec{x}_n \rangle)$$

[数112]

$$b_1, \ldots, b_n \ (\mathrm{resp.}\ \vec{x}_1, \ldots, \vec{x}_n)$$

数１１３に示す基底Ｂと基底Ｂ*とに対して、数１１４である。

[数113]

$$\mathbb{B} := (b_1, \ldots, b_N),$$
$$\mathbb{B}^* := (b_1^*, \ldots, b_N^*)$$

[数114]

$$(x_1,\ldots,x_N)_{\mathbb{B}} := \sum_{i=1}^{N} x_i b_i,$$
$$(y_1,\ldots,y_N)_{\mathbb{B}^*} := \sum_{i=1}^{N} y_i b_i^*$$

[0012] また、以下の説明において、“Ｖｔ”が下付き又は上付きで示されている場合、このＶｔはV_tを意味する。同様に、“δｉ，ｊ”が上付きで示されている場合、このδｉ，ｊは、$\delta_{i,j}$を意味する。同様に、“ｆτ”、“κτ”が上付きで示されている場合、このｆτは、f_τを意味し、このκτはκ_τを意味する。

また、ベクトルを意味する“→”が下付き文字又は上付き文字に付されている場合、この“→”は下付き文字又は上付き文字に上付きで付されていることを意味する。

[0013] また、以下の説明において、暗号処理は、鍵生成処理、暗号化処理、復号処理を含む。

[0014] 実施の形態１．

この実施の形態では、２次スパンプログラムを用いた関数型暗号方式の基礎となる概念と、２次スパンプログラムを用いた関数型暗号方式の概要とを説明する。

第１に、関数型暗号方式を実現するための空間である「双対ペアリングベクトル空間（Ｄｕａｌ　Ｐａｉｒｉｎｇ　Ｖｅｃｔｏｒ　Ｓｐａｃｅｓ，ＤＰＶＳ）」という豊かな数学的構造を有する空間を説明する。

第２に、関数型暗号方式を実現するための概念を説明する。ここでは、「２次スパンプログラム」、「属性情報の等号と２次スパンプログラム」、「秘密分散方式」について説明する。

第３に、２次スパンプログラムを用いた関数型暗号方式の概要について説明する。

[0015] ＜第１．双対ペアリングベクトル空間＞

まず、対称双線形ペアリング群について説明する。

対称双線形ペアリング群（q，G，G_T，g，e）は、素数qと、位数qの巡回加法群Gと、位数qの巡回乗法群G_Tと、g≠0∈Gと、多項式時間で計算可能な非退化双線形ペアリング（Ｎｏｎｄｅｇｅｎｅｒａｔｅ　Ｂｉｌｉｎｅａｒ　Ｐａｉｒｉｎｇ）e：G×G→G_Tとの組である。非退化双線形ペアリングは、e（sg，tg）＝e（g，g）stであり、e（g，g）≠1である。

以下の説明において、G_{bpg}を、1^{λ}を入力として、セキュリティパラメータをλとする双線形ペアリング群のパラメータｐａｒａｍ$_G$：＝（q，G，G_T，g，e）の値を出力するアルゴリズムとする。

[0016] 次に、双対ペアリングベクトル空間について説明する。

双対ペアリングベクトル空間（q，V，G_T，A，e）は、対称双線形ペアリング群（ｐａｒａｍ$_G$：＝（q，G，G_T，g，e））の直積によって構成することができる。双対ペアリングベクトル空間（q，V，G_T，A，e）は、素数q、数１１５に示すF_q上のＮ次元ベクトル空間Ｖ、位数qの巡回群G_T、空間Ｖの標準基底Ａ：＝（a_1，．．．，a_N）の組であり、以下の演算（１）（２）を有する。ここで、a_iは、数１１６に示す通りである。

[数115]

$$\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$$

[数116]

$$a_i := (\overbrace{0,\ldots,0}^{i-1}, g, \overbrace{0,\ldots,0}^{N-i})$$

[0017] 演算（１）：非退化双線形ペアリング

空間Ｖにおけるペアリングは、数１１７によって定義される。

[数117]

$$e(x,y) \coloneqq \prod_{i=1}^{N} e(G_i,H_i) \in \mathbb{G}_T$$

ここで、

$$(G_1,\ldots,G_N) \coloneqq x \in \mathbb{V},$$

$$(H_1,\ldots,H_N) \coloneqq y \in \mathbb{V}$$

である。

これは、非退化双線形である。つまり、ｅ（ｓｘ，ｔｙ）＝ｅ（ｘ，ｙ）stであり、全てのｙ∈Ｖに対して、ｅ（ｘ，ｙ）＝１の場合、ｘ＝０である。また、全てのｉとｊとに対して、ｅ（a_i，a_j）＝ｅ（ｇ，ｇ）$^{\delta i,j}$である。ここで、ｉ＝ｊであれば、$\delta_{i,j}$＝１であり、ｉ≠ｊであれば、$\delta_{i,j}$＝０である。また、ｅ（ｇ，ｇ）≠１∈G_Tである。

[0018] 演算（２）：ディストーション写像

数１１８に示す空間Ｖにおける線形変換$\phi_{i,j}$は、数１１９を行うことができる。

[数118]

$\phi_{i,j}(a_j) = a_i$であり、

$k \neq j$なら、$\phi_{i,j}(a_k) = 0$である。

[数119]

$$\phi_{i,j}(x) \coloneqq (\overbrace{0,\ldots,0}^{i-1}, g_j, \overbrace{0,\ldots,0}^{N-i})$$

ここで、

$$(g_1,\ldots g_N) \coloneqq x$$

である。

ここで、線形変換$\phi_{i,j}$をディストーション写像と呼ぶ。

[0019] 以下の説明において、G_{dpvs}を、1^{λ}（λ∈自然数）、N∈自然数、双線形ペアリング群のパラメータ$param_G:=(q, G, G_T, g, e)$の値を入力として、セキュリティパラメータが$\lambda$であり、N次元の空間Vとする双対ペアリングベクトル空間のパラメータ$param_V:=(q, V, G_T, A, e)$の値を出力するアルゴリズムとする。

[0020] なお、ここでは、上述した対称双線形ペアリング群により、双対ペアリングベクトル空間を構成した場合について説明する。なお、非対称双線形ペアリング群により双対ペアリングベクトル空間を構成することも可能である。以下の説明を、非対称双線形ペアリング群により双対ペアリングベクトル空間を構成した場合に応用することは容易である。

[0021] ＜第２．関数型暗号を実現するための概念＞

＜第２－１．２次スパンプログラム＞

図１は、２次スパンプログラムの説明図である。

体F_qにおける２次スパンプログラムは、２つの多項式の集合$A=\{a_i(x) \mid i\in\{0,...,L\}\}$及び集合$B=\{b_i(x) \mid i\in\{0,...,L\}\}$と、目標多項式d（x）とを含む。また、２次スパンプログラムは、集合$I:=\{1,...,L\}$のラベルρを含む。全てのラベルρ_i（$i=1,...,L$）は、$\{p_0, p_1, ..., p_n, \neg p_1, ..., \neg p_n\}$のいずれか１つのリテラルへ対応付けられる。つまり、$\rho: I\rightarrow\{p_0, p_1, ..., p_n, \neg p_1, ..., \neg p_n\}$である。

[0022] 入力$u:=(u_1, ..., u_n)\in\{0, 1\}^n$に対して、$j=1, ..., n$の各整数jについて、$T(p_j):=u_j$及び$T(\neg p_j):=\neg u_j$により、リテラルの真理値Tが設定される。また、どんな入力uに対しても、p_0の真理値Tは１が設定される。つまり、$T(p_0):=1$である。

集合Iの部分集合I_uは、入力uにより１が設定されたラベルの要素から構成される。つまり、$I_u:=\{i\in I \mid T(p(i)=1)\}$である。又は、$I_u:=\{i\in I \mid [\rho(i)=p_j\wedge u_j=1]\vee[\rho(i)=\neg p_j\wedge u_j=0]\vee[\rho(i)=p_0]\}$である。

[0023] 図２は、部分集合Ｉ$_u$の説明図である。

なお、図２では、ｎ＝７，Ｌ＝６としている。また、図２において、ラベルρは、ρ$_1$が￢ｐ$_2$に、ρ$_2$がｐ$_1$に、ρ$_3$がｐ$_4$に、ρ$_4$が￢ｐ$_5$に、ρ$_5$が￢ｐ$_3$に、ρ$_6$がｐ$_5$にそれぞれ対応付けられているとする。

ここで、入力ｕ：＝（ｕ$_1$，．．．，ｕ$_7$）∈｛０，１｝^{7}が、ｕ$_1$＝１，ｕ$_2$＝０，ｕ$_3$＝１，ｕ$_4$＝０，ｕ$_5$＝０，ｕ$_6$＝１，ｕ$_7$＝１であるとする。この場合、部分集合Ｉ$_u$は、破線で囲んだリテラル（ｐ$_1$，ｐ$_3$，ｐ$_6$，ｐ$_7$，￢ｐ$_2$，￢ｐ$_4$，￢ｐ$_5$）に対応付けられているラベルρ$_i$の要素ｉから構成される。つまり、部分集合Ｉ$_u$は、ラベルρ$_1$，ρ$_2$，ρ$_4$の要素ｉから構成され、部分集合Ｉ$_u$：＝｛ｉ＝１，２，４｝である。

[0024] ２次スパンプログラムは、目標多項式ｄ（ｘ）が数１２０を割り切るような体Ｆ$_q$^{L}における（α$_1$，．．．，α$_L$）及び（β$_1$，．．．，β$_L$）の組であって、部分集合Ｉ$_u$に含まれない全てのｉに対してα$_i$＝０＝β$_i$である（α$_1$，．．．，α$_L$）及び（β$_1$，．．．，β$_L$）の組が存在する場合に限り、入力ｕ∈｛０，１｝^{n}を受理する（又は、部分集合Ｉ$_u$を受理する）。そして、２次スパンプログラムは、他の場合には、入力ｕ∈｛０，１｝^{n}を拒絶する。

[数120]

$$\left(a_0(x)+\sum_{i=1}^{L}\alpha_i\cdot a_i(x)\right)\cdot\left(b_0(x)+\sum_{i=1}^{L}\beta_i\cdot b_i(x)\right)$$

つまり、２次スパンプログラムは、目標多項式ｄ（ｘ）が数１２１を割り切るようなｉ∈Ｉ$_u$についてのα$_i$及びβ$_i$の組が存在する場合に限り、入力ｕ∈｛０，１｝^{n}を受理する。

[数121]

$$\left(a_0(x)+\sum_{i\in\mathcal{I}}\alpha_i\cdot a_i(x)\right)\cdot\left(b_0(x)+\sum_{i\in\mathcal{I}}\beta_i\cdot b_i(x)\right)$$

そして、２次スパンプログラムが入力ｕ∈｛０，１｝^{n}を受理する場合、ｉ∈Ｉ$_{u}$についてのα_{i}及びβ_{i}の組を、多項式時間で計算することが可能である（非特許文献６参照）。

[0025] 図２に示す例であれば、２次スパンプログラムは、目標多項式ｄ（ｘ）が数１２２を割り切るようなｉ∈Ｉ$_{u}$：＝｛ｉ＝１，２，４｝についてのα_{i}及びβ_{i}の組が存在する場合に限り、入力ｕ∈｛０，１｝^{n}を受理する。

[数122]

$$\left(a_0(x)+\sum_{i\in\{1,2,4\}}\alpha_i\cdot a_i(x)\right)\cdot\left(b_0(x)+\sum_{i\in\{1,2,4\}}\beta_i\cdot b_i(x)\right)$$

[0026] ＜第２－２．属性の内積と２次スパンプログラム＞

Ｕ$_{t}$（ｔ＝１，．．．，ｄでありＵ$_{t}$⊂｛０，１｝*）は、部分全集合（ｓｕｂ－ｕｎｉｖｅｒｓｅ）であり、属性の集合である。そして、Ｕ$_{t}$は、それぞれ部分全集合の識別情報（ｔ）と、ｎ次元ベクトルで表された属性情報（$\vec{v}$）とを含む。つまり、Ｕ$_{t}$は、（ｔ，$\vec{v}$）である。ここで、ｔ∈｛１，．．．，ｄ｝であり、$\vec{v}$∈Ｆ$_{q}^{n}$である。

[0027] Ｕ$_{t}$＝（ｔ，$\vec{v}$）をｐとする。つまり、ｐ＝（ｔ，$\vec{v}$）である。ｐ$_{j}$：＝（ｔ，$\vec{v}_{j}$）（ｊ＝１，．．．，ｎ；ｔ∈｛１，．．．，ｄ｝）による２次スパンプログラムＱ：＝（Ａ，Ｂ，ｄ（ｘ），ρ）における、部分集合Ｉ$_{u}$の決定方法について説明する。

アクセスストラクチャＳを、ｐ$_{0}$及び｛ｐ$_{j}$：＝（ｔ，$\vec{v}_{j}$）｝$_{j=1,...,n}$を伴う２次スパンプログラムＱ：＝（Ａ，Ｂ，ｄ（ｘ），ρ）とする。つまり、ρ：｛１，．．．，Ｌ｝→｛ｐ$_{0}$，（ｔ，$\vec{v}_{1}$），．．．，（ｔ，$\vec{v}_{n}$），￢（ｔ，$\vec{v}_{1}$），．．．，￢（ｔ，$\vec{v}_{n}$）｝である。また、Γを属性集合とする。つまり、Γ：＝｛（ｔ，$\vec{x}_{t}$）｜$\vec{x}_{t}$∈Ｆ$_{q}^{n}$，１≦ｔ≦ｄ｝である。ここで、ｔは、｛１，．．．，ｄ｝の部分集合であって、全インデックスである必要はない。

属性集合ΓがアクセスストラクチャSに与えられると、$\{p_0, p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$のリテラルの真理値$T$は次のように決定される。$p_j=(t, v^{\rightarrow}_j)$かつ$(t, x^{\rightarrow}_t)\in\Gamma$かつ$v^{\rightarrow}_j \cdot x^{\rightarrow}_t=0$である場合に限り、$T(p_j):=1$になる。$p_j=\neg(t, v^{\rightarrow}_j)$かつ$(t, x^{\rightarrow}_j)\in\Gamma$かつ$v^{\rightarrow}_j \cdot x^{\rightarrow}_t\neq 0$である場合に限り、$T(\neg p_j):=1$になる。$T(p_0):=1$になる。他の場合には、真理値$T$は0になる。

そして、$I_u(=I_{(\rho,\Gamma)}):=\{i\in I \mid T(\rho(i))=1\}$、つまり、$I_{(\rho,\Gamma)}:=\{i\in I \mid [\rho(i)=(t, v^{\rightarrow}_j)\wedge(t, x^{\rightarrow}_t)\in\Gamma\wedge(v^{\rightarrow}_j \cdot x^{\rightarrow}_t)=0]\vee[\rho(i)=\neg(t, v^{\rightarrow}_j)\wedge(t, x^{\rightarrow}_j)\in\Gamma\wedge v^{\rightarrow}_j \cdot x^{\rightarrow}_t\neq 0]\vee[\rho(i)=p_0]\}$とする。

[0028] ＜第３．関数型暗号方式の概要＞

復号鍵と暗号文との一方に上述したアクセスストラクチャSを持たせ、他方に属性集合Γを持たせることにより、関数型暗号方式を構成する。

[0029] アクセスストラクチャSを復号鍵に持たせた関数型暗号方式をＫｅｙ－Ｐｏｌｉｃｙ関数型暗号（ＫＰ－ＦＥ）方式と呼び、アクセスストラクチャSを暗号文に持たせた暗号方式をＣｉｐｈｅｒｔｅｘｔ－Ｐｏｌｉｃｙ関数型暗号（ＣＰ－ＦＥ）方式と呼ぶ。

ＫＰ－ＦＥ方式及びＣＰ－ＦＥ方式の構成と、各方式を実行する暗号システム１０の構成とを説明する。

[0030] ＜第３－１．ＫＰ－ＦＥ方式＞

ＫＰ－ＦＥ方式は、Ｓｅｔｕｐ、ＫｅｙＧｅｎ、Ｅｎｃ、Ｄｅｃの４つのアルゴリズムを備える。

（Ｓｅｔｕｐ）

Ｓｅｔｕｐアルゴリズムは、セキュリティパラメータλが入力され、公開パラメータｐｋと、マスター鍵ｓｋとを出力する確率的アルゴリズムである。

（ＫｅｙＧｅｎ）

ＫｅｙＧｅｎアルゴリズムは、アクセスストラクチャSと、公開パラメー

タｐｋと、マスター鍵ｓｋとを入力として、復号鍵sk_Sを出力する確率的アルゴリズムである。

（Ｅｎｃ）

Ｅｎｃアルゴリズムは、メッセージｍｓｇと、属性の集合である$\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in F_q^n, 1 \leqq t \leqq d\}$と、公開パラメータｐｋとを入力として、暗号文$ct_\Gamma$を出力する確率的アルゴリズムである。

（Ｄｅｃ）

Ｄｅｃアルゴリズムは、属性の集合であるΓの下で暗号化された暗号文ct_Γと、アクセスストラクチャＳに対する復号鍵sk_Sと、公開パラメータｐｋとを入力として、メッセージｍｓｇ、又は、識別情報$\perp$を出力するアルゴリズムである。

[0031] 図３は、ＫＰ－ＦＥ方式を実行する暗号システム１０の構成図である。

暗号システム１０は、鍵生成装置１００、暗号化装置２００、復号装置３００を備える。

鍵生成装置１００は、セキュリティパラメータλを入力としてＳｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター鍵ｓｋとを生成する。そして、鍵生成装置１００は、生成した公開パラメータｐｋを公開する。また、鍵生成装置１００は、アクセスストラクチャＳを入力としてＫｅｙＧｅｎアルゴリズムを実行して、復号鍵sk_Sを生成して復号装置３００へ秘密裡に配布する。

暗号化装置２００は、メッセージｍｓｇと、属性の集合Γと、公開パラメータｐｋとを入力としてＥｎｃアルゴリズムを実行して、暗号文ct_Γを生成する。暗号化装置２００は、生成した暗号文ct_Γを復号装置３００へ送信する。

復号装置３００は、公開パラメータｐｋと、復号鍵sk_Sと、暗号文ct_Γとを入力としてＤｅｃアルゴリズムを実行して、メッセージｍｓｇ又は識別情報$\perp$を出力する。

[0032] ＜第３－２．ＣＰ－ＦＥ方式＞

ＣＰ－ＦＥ方式は、Ｓｅｔｕｐ、ＫｅｙＧｅｎ、Ｅｎｃ、Ｄｅｃの４つのアルゴリズムを備える。

（Ｓｅｔｕｐ）

Ｓｅｔｕｐアルゴリズムは、セキュリティパラメータλが入力され、公開パラメータｐｋと、マスター鍵ｓｋとを出力する確率的アルゴリズムである。

（ＫｅｙＧｅｎ）

ＫｅｙＧｅｎアルゴリズムは、属性の集合である$\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in F_q^n, 1 \leqq t \leqq d\}$と、公開パラメータｐｋと、マスター鍵ｓｋとを入力として、復号鍵sk_Γを出力する確率的アルゴリズムである。

（Ｅｎｃ）

Ｅｎｃアルゴリズムは、メッセージｍｓｇと、アクセスストラクチャＳと、公開パラメータｐｋとを入力として、暗号文ct_Sを出力する確率的アルゴリズムである。

（Ｄｅｃ）

Ｄｅｃアルゴリズムは、アクセスストラクチャＳの下で暗号化された暗号文ct_Sと、属性の集合であるΓに対する復号鍵sk_Γと、公開パラメータｐｋとを入力として、メッセージｍｓｇ、又は、識別情報⊥を出力するアルゴリズムである。

[0033] 図４は、ＣＰ－ＦＥ方式を実行する暗号システム１０の構成図である。

暗号システム１０は、鍵生成装置１００、暗号化装置２００、復号装置３００を備える。

鍵生成装置１００は、セキュリティパラメータλを入力としてＳｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター鍵ｓｋとを生成する。そして、鍵生成装置１００は、生成した公開パラメータｐｋを公開する。また、鍵生成装置１００は、属性の集合Γを入力としてＫｅｙＧｅｎアルゴリズムを実行して、復号鍵sk_Γを生成して復号装置３００へ秘密裡に配布する。

暗号化装置２００は、メッセージｍｓｇと、アクセスストラクチャＳと、公開パラメータｐｋとを入力としてＥｎｃアルゴリズムを実行して、暗号文ct_Sを生成する。暗号化装置２００は、生成した暗号文ct_Sを復号装置３００へ送信する。

復号装置３００は、公開パラメータｐｋと、復号鍵sk_Γと、暗号文ct_Sとを入力としてＤｅｃアルゴリズムを実行して、メッセージｍｓｇ又は識別情報⊥を出力する。

[0034] ＫＰ－ＦＥ方式及びＣＰ－ＦＥ方式のどちらにおいても、Ｄｅｃアルゴリズムでは、アクセスストラクチャＳと属性集合Γとに基づき、上述した方法により、部分集合$I_{(\rho,\Gamma)}$を選択し、さらに係数（α_1，．．．，α_L）及び係数（β_1，．．．，β_L）を特定する。そして、部分集合$I_{(\rho,\Gamma)}$と係数（α_1，．．．，α_L）及び係数（β_1，．．．，β_L）とに基づき、暗号文ct_Γ（又はct_S）を復号してメッセージｍｓｇを計算する。

[0035] なお、Ｓｅｔｕｐアルゴリズムは、通常、システムのセットアップ時に１度だけ実行される。ＫｅｙＧｅｎアルゴリズムは、ユーザの復号鍵を生成する度に実行される。Ｅｎｃアルゴリズムは、メッセージｍｓｇを暗号化する度に実行される。Ｄｅｃアルゴリズムは、暗号文を復号する度に実行される。

[0036] 実施の形態１に係る暗号システム１０では、２次スパンプログラムに基づくアクセスストラクチャＳを用いて関数型暗号方式を構成する。これにより、関係Ｒとして表現できる範囲を理想化された範囲とすることが可能となる。

[0037] 実施の形態２．

実施の形態２では、２次スパンプログラムを用いた関数型暗号方式の構成例について説明する。

ここでは、ＫＰ－ＦＥ方式を例として説明する。

[0038] 図５は、実施の形態２に係る鍵生成装置１００の構成図である。図６は、実施の形態２に係る暗号化装置２００の構成図である。図７は、実施の形態

２に係る復号装置３００の構成図である。

図８と図９とは、鍵生成装置１００の動作を示すフローチャートである。図８はＳｅｔｕｐアルゴリズムの処理を示すフローチャートであり、図９はＫｅｙＧｅｎアルゴリズムの処理を示すフローチャートである。図１０は、暗号化装置２００の動作を示すフローチャートであり、Ｅｎｃアルゴリズムの処理を示すフローチャートである。図１１は、復号装置３００の動作を示すフローチャートであり、Ｄｅｃアルゴリズムの処理を示すフローチャートである。

[0039] 鍵生成装置１００の機能と動作とについて説明する。

鍵生成装置１００は、マスター鍵生成部１１０、マスター鍵記憶部１２０、情報入力部１３０、復号鍵生成部１４０、鍵配布部１５０を備える。また、復号鍵生成部１４０は、秘密情報生成部１４１、鍵要素生成部１４２を備える。

[0040] 図８に基づき、Ｓｅｔｕｐアルゴリズムの処理について説明する。

（Ｓ１０１：正規直交基底生成ステップ）

マスター鍵生成部１１０は、処理装置により、数１２３を計算して、パラメータｐａｒａｍと、基底B_0及び基底B^*_0と、基底B_t及び基底B^*_tとを生成する。

[数123]

(1) input 1^{λ}

(2) $\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, g, e) \xleftarrow{R} \mathcal{G}_{\mathrm{bpg}}(1^{\lambda})$

(3) $\psi \xleftarrow{U} \mathbb{F}_q^{\times}$

(4) $n_0 := 2mf_{\mathsf{max}} + 1,$

$n_t := 2mf_{\mathsf{max}}k_{\mathsf{max}} + n \ (t = 1, ..., d),$

$N_0 := n_0 + u_0 + w_0 + z_0,$

$N_t := n_t + u_t + w_t + z_t \ (t = 1, ..., d)$

t＝0,...，dの各tについて（5）から（9）の処理を実行する。

(5) $\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda}, N_t, \mathsf{param}_{\mathbb{G}})$

(6) $X_t := (\chi_{t,i,j})_{i,j=1,...,N_t} \xleftarrow{U} GL(N_t, \mathbb{F}_q)$

(7) $X_t^* := (\vartheta_{t,i,j})_{i,j=1,...,N_t} := \psi \cdot (X_t^T)^{-1}$

(8) $\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j}\boldsymbol{a}_{t,j} \ \text{ for } i = 1, ..., N_t,$

$\mathbb{B}_t := (\boldsymbol{b}_{t,1}, ..., \boldsymbol{b}_{t,N_t})$

(9) $\boldsymbol{b}_{t,i}^* := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \vartheta_{t,i,j}\boldsymbol{a}_{t,j} \ \text{ for } i = 1, ..., N_t,$

$\mathbb{B}_t^* := (\boldsymbol{b}_{t,1}^*, ..., \boldsymbol{b}_{t,N_t}^*)$

(10) $g_T := e(g, g)^{\psi},$

$\mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,...,d}, g_T)$

[0041] つまり、マスター鍵生成部１１０は以下の処理を実行する。

（１）マスター鍵生成部１１０は、入力装置により、セキュリティパラメータλ（1^{λ}）を入力する。

（２）マスター鍵生成部１１０は、処理装置により、（１）で入力したセ

キュリティパラメータλを入力としてアルゴリズムG_{bpg}を実行して、双線形ペアリング群のパラメータ$param_G:=(q, G, G_T, g, e)$の値を生成する。

（３）マスター鍵生成部１１０は、処理装置により、乱数φを生成する。

（４）マスター鍵生成部１１０は、N_0に$n_0+u_0+w_0+z_0$を設定し、$t=1,\ldots,d$（ｄは１以上の整数）の各整数ｔについて、N_tに$n_t+u_t+w_t+z_t$を設定する。ここで、n_0は$2mf_{max}+1$であり、n_tは$2mf_{max}k_{max}+n$である。ｍは、目標多項式ｄ（ｘ）を因数分解した場合の因数の数である。f_{max}は、目標多項式ｄ（ｘ）を因数分解した場合の因数の次数の最大値（後述するf_τの最大値）である。k_{max}は、１つの識別情報ｔに対応付けられるラベルρの個数の最大値である。ｎは１以上の整数であり、u_0，w_0，z_0，u_t，w_t，z_tはそれぞれ０以上の整数である。

[0042] 続いて、マスター鍵生成部１１０は、ｔ＝０，．．．，ｄの各整数ｔについて以下の（５）から（９）までの処理を実行する。

（５）マスター鍵生成部１１０は、処理装置により、（１）で入力したセキュリティパラメータλと、（４）で設定したN_tと、（２）で生成した$param_G:=(q, G, G_T, g, e)$の値とを入力としてアルゴリズム$G_{dpvs}$を実行して、双対ペアリングベクトル空間のパラメータ$param_{Vt}:=(q, V_t, G_T, A_t, e)$の値を生成する。

（６）マスター鍵生成部１１０は、処理装置により、（４）で設定したN_tと、F_qとを入力として、線形変換$X_t:=(\chi_{t,i,j})_{i,j}$をランダムに生成する。なお、ＧＬは、Ｇｅｎｅｒａｌ　Ｌｉｎｅａｒの略である。つまり、ＧＬは、一般線形群であり、行列式が０でない正方行列の集合であり、乗法に関し群である。また、$(\chi_{t,i,j})_{i,j}$は、行列$\chi_{t,i,j}$の添え字ｉ，ｊに関する行列という意味であり、ここでは、ｉ，ｊ＝１，．．．，N_tである。

（７）マスター鍵生成部１１０は、処理装置により、乱数φと線形変換X_tとに基づき、$X^*_t:=(\nu_{t,i,j})_{i,j}:=\phi\cdot(X_t^T)^{-1}$を生成する。なお、$(\nu_{t,i,j})_{i,j}$も$(\chi_{t,i,j})_{i,j}$と同様に、行列$\nu_{t,i,j}$の添え字ｉ

，ｊに関する行列という意味であり、ここでは、ｉ，ｊ＝１，．．．．，N_tである。

（８）マスター鍵生成部１１０は、処理装置により、（６）で生成した線形変換X_tに基づき、（５）で生成した標準基底A_tから基底B_tを生成する。なお、$\vec{x}_{t,i}$とは、線形変換X_tのｉ行目を示す。

（９）マスター鍵生成部１１０は、処理装置により、（７）で生成した線形変換X^*_tに基づき、（５）で生成した標準基底A_tから基底B^*_tを生成する。なお、$\vec{v}_{t,i}$とは、線形変換X^*_tのｉ行目を示す。

（１０）マスター鍵生成部１１０は、処理装置により、g_Tにｅ（ｇ，ｇ）$^{\psi}$を設定する。また、マスター鍵生成部１１０は、ｐａｒａｍに（５）で生成した$\{param_{Vt}\}_{t=0,...,d}$と、$g_T$とを設定する。

[0043] すなわち、（Ｓ１０１）で、マスター鍵生成部１１０は、数１２４に示すアルゴリズムG_{ob}を実行して、ｐａｒａｍと、基底B_0及び基底B^*_0と、基底B_t及び基底B^*_tとを生成する。

[数124]

$$\mathcal{G}_{\mathrm{ob}}(1^{\lambda}):$$

$$\mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,g,e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathrm{bpg}}(1^{\lambda}),\ \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times},$$

$$n_0 := 2mf_{\mathsf{max}}+1,\quad n_t := 2mf_{\mathsf{max}}k_{\mathsf{max}}+n\ (t=1,...,d),$$

$$N_0 := n_0+u_0+w_0+z_0,\ N_t := n_t+u_t+w_t+z_t\ (t=1,...,d),$$

for $t=0,...,d$,

$$\mathsf{param}_{\mathbb{V}_t} := (q,\mathbb{V}_t,\mathbb{G}_T,\mathbb{A}_t,e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t,\mathsf{param}_{\mathbb{G}}),$$

$$X_t := (\chi_{t,i,j})_{i,j=1,..,N_t} \xleftarrow{\mathsf{U}} GL(N_t,\mathbb{F}_q),$$

$$X_t^* := (\vartheta_{t,i,j})_{i,j=1,..,N_t} := \psi\cdot(X_t^T)^{-1},\ \text{hereafter, } \vec{\chi}_{t,i}$$

and $\vec{\vartheta}_{t,i}$ denote the i-th rows of X_t and X_t^* for $i=1,...,N_t$, respectively,

$$\boldsymbol{b}_{t,i} := (\vec{\chi}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t}\chi_{t,i,j}\boldsymbol{a}_{t,j}\ \text{ for } i=1,...,N_t,\ \mathbb{B}_t := (\boldsymbol{b}_{t,1},...,\boldsymbol{b}_{t,N_t}),$$

$$\boldsymbol{b}_{t,i}^* := (\vec{\vartheta}_{t,i})_{\mathbb{A}_t} = \sum_{j=1}^{N_t}\vartheta_{t,i,j}\boldsymbol{a}_{t,j}\ \text{ for } i=1,...,N_t,\ \mathbb{B}_t^* := (\boldsymbol{b}_{t,1}^*,...,\boldsymbol{b}_{t,N_t}^*),$$

$$g_T := e(g,g)^{\psi},\ \mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,...,d},g_T),$$

return $(\mathsf{param},\mathbb{B}_t,\mathbb{B}_t^*)$.

[0044] （Ｓ１０２：公開パラメータ生成ステップ）

マスター鍵生成部１１０は、処理装置により、（Ｓ１０１）で生成した基底Ｂ$_0$の部分基底Ｂ＾$_0$と、基底Ｂ$_t$の部分基底Ｂ＾$_t$とを数１２５に示すように生成する。

[数125]

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1},\boldsymbol{b}_{0,n_0+u_0+w_0+1},...,\boldsymbol{b}_{0,n_0+u_0+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1},...,\boldsymbol{b}_{t,n},\boldsymbol{b}_{t,n_t+u_t+w_t+1},...,\boldsymbol{b}_{t,n_t+u_t+w_t+z_t})\quad \text{for } t=1,..,d$$

マスター鍵生成部１１０は、生成した部分基底Ｂ＾$_0$及び部分基底Ｂ＾$_t$と、（Ｓ１０１）で入力されたセキュリティパラメータλと、（Ｓ１０１）で生成したｐａｒａｍとを合わせて、公開パラメータｐｋとする。

[0045] （Ｓ１０３：マスター鍵生成ステップ）

マスター鍵生成部１１０は、処理装置により、（Ｓ１０１）で生成した基底Ｂ＊$_0$の部分基底Ｂ＾＊$_0$と、基底Ｂ＊$_t$の部分基底Ｂ＾＊$_t$とを数１２６に示すように生成する。

[数126]

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*,\ldots,\boldsymbol{b}_{0,n_0}^*,\boldsymbol{b}_{0,n_0+u_0+1}^*,\ldots,\boldsymbol{b}_{0,n_0+u_0+w_0}^*,\boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^*),$$
$$\hat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*,\ldots,\boldsymbol{b}_{t,n_t}^*,\boldsymbol{b}_{t,n_t+u_t+1}^*,\ldots,\boldsymbol{b}_{t,n_t+u_t+w_t}^*) \quad \text{for } t=1,..,d$$

マスター鍵生成部１１０は、生成した部分基底Ｂ＾＊$_0$と部分基底Ｂ＾＊$_t$とをマスター鍵ｓｋとする。

[0046] （Ｓ１０４：マスター鍵記憶ステップ）

マスター鍵記憶部１２０は、（Ｓ１０２）で生成した公開パラメータｐｋを記憶装置に記憶する。また、マスター鍵記憶部１２０は、（Ｓ１０３）で生成したマスター鍵ｓｋを記憶装置に記憶する。

[0047] つまり、（Ｓ１０１）から（Ｓ１０３）において、鍵生成装置１００は、数１２７に示すＳｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター鍵ｓｋとを生成する。そして、（Ｓ１０４）で、鍵生成装置１００は、生成した公開パラメータｐｋとマスター鍵ｓｋとを記憶装置に記憶する。

なお、公開パラメータは、例えば、ネットワークを介して公開され、暗号化装置２００や復号装置３００が取得可能な状態にされる。

[数127]

$$\mathrm{Setup}(1^{\lambda}):$$

$$(\mathrm{param}, (\mathbb{B}_t, \mathbb{B}_t^*)_{t=0,\ldots,d}) \xleftarrow{R} \mathcal{G}_{\mathrm{ob}}(1^{\lambda})$$

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}) \quad \text{for } t = 1,..,d,$$

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \ldots, \boldsymbol{b}_{0,n_0}^*, \boldsymbol{b}_{0,n_0+u_0+1}^*, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^*, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^*),$$

$$\hat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,n_t+u_t+1}^*, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^*) \quad \text{for } t = 1,..,d,$$

$$\text{return } \mathrm{pk} := (1^{\lambda}, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \mathrm{param}), \quad \mathrm{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}.$$

[0048] 図９に基づき、ＫｅｙＧｅｎアルゴリズムの処理について説明する。

（Ｓ２０１：情報入力ステップ）

情報入力部１３０は、入力装置により、上述したアクセスストラクチャＳ：＝（Ａ，Ｂ，ｄ（ｘ），ρ）を入力する。なお、ρは、例えば、復号鍵ｓｋ$_S$の使用者の属性情報が設定されている。また、アクセスストラクチャＳに含まれる目標多項式ｄ（ｘ）は、数１２８に示すように、τ＝１，．．．，ｍのｍ個の因数ｄ$_\tau$（ｘ）$^{f_\tau}$に因数分解可能である。

[数128]

$$d(x) = \prod_{\tau=1}^{m} d_\tau(x)^{f_\tau}$$

[0049] （Ｓ２０２：秘密情報π生成ステップ）

秘密情報生成部１４１は、処理装置により、秘密情報$\pi_{\tau,\kappa,0}$及び秘密情報$\pi_{\tau,\kappa,1}$を数１２９に示すように生成する。

[数129]

$$\pi_\tau \xleftarrow{U} \mathbb{F}_q,\ (\tau = 1,...,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1} \pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau = 1,...,m;\ \ \kappa = 0,...,f_\tau)$$

[0050] （Ｓ２０３：秘密情報χ生成ステップ）

秘密情報生成部１４１は、処理装置により、秘密情報$\chi_{\tau,\kappa,0}$及び秘密情報$\chi_{\tau,\kappa,1}$を数１３０に示すように生成する。

[数130]

$$\chi_\tau \xleftarrow{U} \mathbb{F}_q,\ (\tau = 1,...,m-1),\ \ \chi_m := 1 - \sum_{\tau=1}^{m-1} \chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{U} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau = 1,...,m;\ \ \kappa = 0,...,f_\tau)$$

[0051] （Ｓ２０４：秘密情報ｓ生成ステップ）

秘密情報生成部１４１は、処理装置により、秘密情報$s_0^{(\tau,\kappa,0)}$及び秘密情報$s_0^{(\tau,\kappa,1)}$と、秘密情報$s_i^{(\tau,\kappa,0)}$及び秘密情報$s_i^{(\tau,\kappa,1)}$とを数１３１に示すように生成する。

[数131]

$$\text{for } \tau = 1,\ldots,m,\ \ \kappa = 0,\ldots,f_\tau,\ \ \iota = 0,1,$$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa = 0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\cup} \mathbb{F}_q,\ \left(j = 0,\ldots,\mu^{(\tau,\kappa,\iota)}-1\right),$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

$$\text{for } i = 1,\ldots,L,$$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \left(i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1\right),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\left(i = 1,\ldots,L;\ \iota = 0,1\right),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1}$$

[0052] （Ｓ２０５：鍵要素生成ステップ）

鍵要素生成部１４２は、処理装置により、τ＝１，．．．，ｍの各整数τと、κ＝０，．．．，ｆ$_\tau$の各整数κと、ι＝０，１の各整数ιとについて、復号鍵ｓｋ$_S$の要素ｋ$*_{0}^{(\tau,\kappa,\iota)}$を数１３２に示すように生成する。

[数132]

$$\vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}, \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0}, \overbrace{0,\ldots,0}^{u_0}, \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0}, \overbrace{0,\ldots,0, \chi_{\tau,\kappa,\iota}}^{z_0}) \mathbb{B}_0^*$$

なお、上述したように、数１１３に示す基底Ｂと基底Ｂ*とに対して、数１１４である。したがって、数１３２は、基底Ｂ*$_0$の基底ベクトルｂ*$_{0,1}$の係数としてｓ$_0^{(\tau,\kappa,\iota)}$＋$\pi_{\tau,\kappa,\iota}$を設定し、基底ベクトルｂ*$_{0,1+1}$，．．．，ｂ*$_{0,1+n0}$の係数としてｅ→$_0^{(\tau,\kappa,\iota)}$を設定し、基底ベクトルｂ*$_{0,n0+1}$，．．．，ｂ*$_{0,n0+u0}$の係数として０を設定し、基底ベクトルｂ*$_{0,n0+u0+1}$，．．．，ｂ*$_{0,n0+u0+w0}$の係数として$\eta_{0,1}^{(\tau,\kappa,\iota)}$，．．．，$\eta_{0,w0}^{(\tau,\kappa,\iota)}$を設定し、基底ベクトルｂ*$_{0,n0+u0+w0+1}$，．．．，ｂ*$_{0,n0+u0+w0+z0}$の係数として０を設定することを意味する。ここで、ｎ０，ｕ０，ｗ０，ｚ０はそれぞれｎ$_0$，ｕ$_0$，ｗ$_0$，ｚ$_0$のことである。

また、ｅ→$_0^{(\tau,\kappa,\iota)}$は、１つの基底ベクトルの係数として１が設定され、他の基底ベクトルの係数として０が設定された２ｍｆ$_{max}$次元のベクトルであって、係数として１が設定される基底ベクトルが（τ，κ，ι）毎に異なるベクトルである。同様に、ｅ→$_i^{(\tau,\kappa,\iota)}$は、１つの基底ベクトルの係数として１が設定され、他の基底ベクトルの係数として０が設定された２ｍｆ$_{max}$ｋ$_{max}$次元のベクトルであって、係数として１が設定される基底ベクトルが（τ，κ，ι）毎に異なるベクトルである。

また、ｅ→$_1$は、基底ベクトルｂ*$_{t,1}$の係数として１が設定され、他の基底ベクトルの係数として０が設定されたｎ次元のベクトルである。

鍵要素生成部１４２は、処理装置により、τ＝１，．．．，ｍの各整数τと、κ＝０，．．．，ｆ$_\tau$の各整数κと、ι＝０，１の各整数ιと、ｉ＝１，．．．，Ｌの各整数ｉとについて、復号鍵ｓｋ$_S$の要素ｋ*$_i^{(\tau,\kappa,\iota)}$を数１３３に示すように生成する。

[数133]

$$\text{if } \rho(i)=(t,\vec{v}_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1+\theta_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{if } \rho(i)=\neg(t,\vec{v}_i),\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{if } \rho(i)=p_0,\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_i}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*$$

[0053] （Ｓ２０６：鍵配布ステップ）

鍵配布部１５０は、（Ｓ２０１）で入力したアクセスストラクチャＳと、（Ｓ２０５）で生成されたｋ＊$_0{}^{(\tau,\kappa,\iota)}$，ｋ＊$_1{}^{(\tau,\kappa,\iota)}$，．．．，ｋ＊$_L{}^{(\tau,\kappa,\iota)}$とを要素とする復号鍵ｓｋ$_S$を、例えば通信装置によりネットワークを介して秘密裡に復号装置３００へ配布する。もちろん、復号鍵ｓｋ$_S$は、他の方法により復号装置３００へ配布されてもよい。

[0054] つまり、（Ｓ２０１）から（Ｓ２０５）において、鍵生成装置１００は、数１３４から数１３５に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵ｓｋ$_S$を生成する。そして、（Ｓ２０６）で、鍵生成装置１００は、生成した復号鍵ｓｋ$_S$を復号装置３００へ配布する。

[数134]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \ \kappa=0,\ldots,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x+\cdots+a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x+\cdots+b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (j=0,\ldots,\mu^{(\tau,\kappa,\iota)}-1),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1}\delta_j^{(\tau,\kappa,0)}\cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1}\delta_j^{(\tau,\kappa,1)}\cdot b_{0,j}^{(\tau,\kappa)},$$

[数135]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0},\ \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^*,$$

for $i = 1,...,L$,

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i = 1,...,L;\ \tau = 1,...,m-1;\iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i = 1,...,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

if $\rho(i) = (t, \vec{v}_i)$, $\quad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i \vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^*,$$

if $\rho(i) = \neg(t, \vec{v}_i)$, $\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^*,$$

if $\rho(i) = p_0$, $\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\eta}_i,}^{w_0}\ \overbrace{0,...,0}^{z_0})\ \mathbb{B}_0^*,$$

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1})$.

[0055] 暗号化装置２００の機能と動作とについて説明する。

暗号化装置２００は、公開パラメータ取得部２１０、情報入力部２２０、暗号化データ生成部２３０、データ送信部２４０を備える。

[0056] 図１０に基づき、Ｅｎｃアルゴリズムの処理について説明する。

（Ｓ３０１：公開パラメータ取得ステップ）

公開パラメータ取得部２１０は、例えば、通信装置によりネットワークを介して、鍵生成装置１００が生成した公開パラメータｐｋを取得する。

[0057] （Ｓ３０２：情報入力ステップ）

情報入力部２２０は、入力装置により、復号装置３００へ送信するメッセージｍｓｇを入力する。また、情報入力部２２０は、入力装置により、属性の集合Γ：＝｛（ｔ，$\vec{x}_t$：＝（$x_{t,1}$，．．．，$x_{t,n}\in\mathbb{F}_q^n$））｜１≦ｔ≦ｄ｝を入力する。なお、ｔは、１以上ｄ以下の全ての整数ではなく、１以上ｄ以下の少なくとも一部の整数であってもよい。また、属性の集合Γは、例えば、復号可能なユーザの属性情報が設定されている。

[0058] （Ｓ３０３：暗号要素生成ステップ）

暗号化データ生成部２３０は、処理装置により、暗号文ct_Γの要素c_0を数１３６に示すように生成する。

[数136]

$$\omega,\zeta \xleftarrow{U} \mathbb{F}_q,$$
$$\vec{\varphi}_0 \xleftarrow{U} \mathbb{F}_q^{z_0-1},$$
$$c_0 := (\overbrace{\omega, 0,...,0,}^{n_0}\overbrace{0,...,0,}^{u_0}\overbrace{0,...,0,}^{w_0}\overbrace{\vec{\varphi}_0, \zeta}^{z_0})\,\mathbb{B}_0$$

暗号化データ生成部２３０は、処理装置により、属性情報Γに含まれる各整数ｔについて、暗号文ct_Γの要素c_tを数１３７に示すように生成する。

[数137]

$$\vec{\varphi}_t \xleftarrow{U} \mathbb{F}_q^{z_t} \text{ for } (t,\vec{x}_t)\in\Gamma,$$
$$c_t := (\overbrace{\omega\vec{x}_t, 0,...,0}^{n_t}\overbrace{0,...,0,}^{u_t}\overbrace{0,...,0,}^{w_t}\overbrace{\vec{\varphi}_t}^{z_t})\,\mathbb{B}_t$$

暗号化データ生成部２３０は、処理装置により、暗号文ct_Γの要素c_{d+1}を数１３８に示すように生成する。

[数138]

$$c_{d+1} := g_T^{\zeta} msg$$

[0059] （Ｓ３０４：データ送信ステップ）

データ送信部２４０は、（Ｓ３０２）で入力した属性の集合Γと、（Ｓ３０３）で生成されたｃ$_0$，ｃ$_t$，ｃ$_{d+1}$とを要素とする暗号文ｃｔ$_\Gamma$を、例えば通信装置によりネットワークを介して復号装置３００へ送信する。もちろん、暗号文ｃｔ$_\Gamma$は、他の方法により復号装置３００へ送信されてもよい。

[0060] つまり、（Ｓ３０１）から（Ｓ３０３）において、暗号化装置２００は、数１３９に示すＥｎｃアルゴリズムを実行して、暗号文ｃｔ$_\Gamma$を生成する。そして、（Ｓ３０４）で、暗号化装置２００は生成した暗号文ｃｔ$_\Gamma$を復号装置３００へ送信する。

[数139]

$$\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, msg, \Gamma := \{(t,\vec{x}_t) \mid 1 \le t \le d\}):\\
&\omega, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},\\
&\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t} \text{ for } (t,\vec{x}_t) \in \Gamma,\\
&\boldsymbol{c}_0 := (\overbrace{\omega,\ 0,...,0,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...,0,}^{w_0}\ \overbrace{\vec{\varphi}_0,\ \zeta}^{z_0})\,\mathbb{B}_0\ ,\\
&\boldsymbol{c}_t := (\overbrace{\omega\vec{x}_t,\ 0,...,0}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\varphi}_t}^{z_t})\,\mathbb{B}_t\ ,\ \text{for } (t,\vec{x}_t) \in \Gamma,\\
&c_{d+1} := g_T^{\zeta} msg,\\
&\text{return } \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\vec{x}_t)\in\Gamma}, c_{d+1}).
\end{aligned}$$

[0061] 復号装置３００の機能と動作とについて説明する。

復号装置３００は、情報取得部３１０、スパンプログラム計算部３２０、補完係数計算部３３０、復号部３４０を備える。また、情報取得部３１０は

、復号鍵取得部３１１、暗号文取得部３１２を備える。また、補完係数計算部３３０は、多項式選択部３３１、係数計算部３３２を備える。また、復号部３４０は、ペアリング演算部３４１、メッセージ計算部３４２を備える。

[0062] 図１１に基づき、Ｄｅｃアルゴリズムの処理について説明する。

（Ｓ４０１：復号鍵取得ステップ）

復号鍵取得部３１１は、例えば、通信装置によりネットワークを介して、鍵生成装置１００から配布された復号鍵sk_S：＝（Ｓ，$k^*_{0}{}^{(\tau,\kappa,\iota)}$，$k^*_{1}{}^{(\tau,\kappa,\iota)}$，．．．，$k^*_{L}{}^{(\tau,\kappa,\iota)}$）を取得する。また、復号鍵取得部３１１は、鍵生成装置１００が生成した公開パラメータｐｋを取得する。

[0063] （Ｓ４０２：暗号文取得ステップ）

暗号文取得部３１２は、例えば、通信装置によりネットワークを介して、暗号化装置２００が送信した暗号文ct_Γ：＝（Γ，c_0，c_t，c_{d+1}）を取得する。

[0064] （Ｓ４０３：スパンプログラム計算ステップ）

スパンプログラム計算部３２０は、処理装置により、（Ｓ４０１）で取得した復号鍵sk_Sに含まれるアクセスストラクチャＳが、（Ｓ４０２）で取得した暗号文ct_Γに含まれるΓを受理するか否かを判定する。アクセスストラクチャＳがΓを受理するか否かの判定方法は、「実施の形態１における第２－１．２次スパンプログラム」で説明した通りである。

スパンプログラム計算部３２０は、アクセスストラクチャＳがΓを受理する場合（Ｓ４０３で受理）、処理を（Ｓ４０４）へ進める。一方、アクセスストラクチャＳがΓを拒絶する場合（Ｓ４０３で拒絶）、暗号文ct_Γを復号鍵sk_Sで復号できないとして処理を終了する。

[0065] （Ｓ４０４：多項式選択ステップ）

補完係数計算部３３０の多項式選択部３３１は、処理装置により、$I_{(\rho,\Gamma)} \subseteq \{1,．．．,L\}$を計算する。$I_{(\rho,\Gamma)}$の計算方法は、「実施の形態１の第２－２．属性の内積と２次スパンプログラム」で説明した通りである。

[0066] （Ｓ４０５：係数計算ステップ）

補完係数計算部３３０の係数計算部３３２は、処理装置により、数１４０となる係数（$\alpha_1, \ldots, \alpha_L$）と、係数（$\beta_1, \ldots, \beta_L$）と、次数（$\kappa_1, \ldots, \kappa_m$）とを計算する。係数（$\alpha_1, \ldots, \alpha_L$）と、係数（$\beta_1, \ldots, \beta_L$）と、次数（$\kappa_1, \ldots, \kappa_m$）との計算方法は、どのような方法でもよく、例えば総当たり法により計算してもよい。

[数140]

$$\prod_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x)), \text{ and}$$
$$\prod_{\tau=1}^{m} d_\tau(x)^{f\tau-\kappa_\tau} \mid (b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x))$$

ここで、$I_{(\rho, \Gamma)}$に含まれない全てのｉについては、$\alpha_i = 0 = \beta_i$である。

[0067] （Ｓ４０６：ペアリング演算ステップ）

復号部３４０のペアリング演算部３４１は、処理装置により、数１４１を計算して、セッション鍵$K_{\tau, 0}$，$K_{\tau, 1}$を生成する。

[数141]

$$K_{\tau,0} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$
$$\cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)},$$
$$K_{\tau,1} := e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$
$$\cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i \in \mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(\vec{v}_i \cdot \vec{x}_t)},$$
$$\text{where } \mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\},$$
$$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t, \vec{v}_i)\} \text{ and}$$
$$\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t, \vec{v}_i)\}$$

[0068] （Ｓ４０７：メッセージ計算ステップ）

復号部３４０のメッセージ計算部３４２は、処理装置により、数１４２を計算して、メッセージｍｓｇ’（＝ｍｓｇ）を生成する。

[数142]

$$msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1})$$

なお、数１４３に示すように、数１４１を計算することによりｇ$_{T}{}^{\zeta}$が得られる。そのため、数１４２を計算することにより、メッセージｍｓｇ’（＝ｍｓｇ）を得られる。

[数143]

$$
\begin{aligned}
K_{\tau,0} &:= e(\boldsymbol{c}_0, \boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \\
&\quad \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)}, \\
&= g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}a_{0,j}^{(\tau,\kappa_\tau)}+\pi_{\tau,\kappa_\tau,0})+\zeta\chi_{\tau,\kappa_\tau,0}} \\
&\quad \cdot g_T^{\omega(\sum_{i=1}^{L}\alpha_i\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}a_{i,j}^{(\tau,\kappa_\tau)}+\xi_{i,\tau,0}))} \\
&= g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}a_{0,j}^{(\tau,\kappa_\tau)}+\pi_{\tau,\kappa_\tau,0})+\zeta\chi_{\tau,\kappa_\tau,0}} \\
&\quad \cdot g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}\sum_{i=1}^{L}\alpha_i a_{i,j}^{(\tau,\kappa_\tau)}+\alpha_i\xi_{i,\tau,0})} \\
&= g_T^{\omega(\sum_{j=0}^{\mu(\tau,\kappa_\tau,0)-1}\delta_j^{(\tau,\kappa_\tau,0)}(a_{0,j}^{(\tau,\kappa_\tau)}+\sum_{i=1}^{L}\alpha_i a_{i,j}^{(\tau,\kappa_\tau)})} \\
&\quad \cdot g_T^{\omega\pi_{\tau,\kappa_\tau,0}+\zeta\chi_{\tau,\kappa_\tau,0}+\omega\sum_{i=1}^{L}\alpha_i\xi_{i,\tau,0}} \\
&= g_T^{\omega\pi_{\tau,\kappa_\tau,0}+\zeta\chi_{\tau,\kappa_\tau,0}+\omega\sum_{i=1}^{L}\alpha_i\xi_{i,\tau,0}} \\
K_{\tau,1} &= g_T^{\omega\pi_{\tau,\kappa_\tau,1}+\zeta\chi_{\tau,\kappa_\tau,1}+\omega\sum_{i=1}^{L}\beta_i\xi_{i,\tau,1}} \\
\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1} &= g_T^{\sum_{\tau=1}^{m}(\omega(\pi_{\tau,\kappa_\tau,0}+\pi_{\tau,\kappa_\tau,1})+\zeta(\chi_{\tau,\kappa_\tau,0}+\chi_{\tau,\kappa_\tau,1})+\omega\sum_{i=1}^{L}(\alpha_i\xi_{i,\tau,0}+\beta_i\xi_{i,\tau,1}))} \\
&= g_T^{\omega(\sum_{\tau=1}^{m}\pi_\tau+\zeta\sum_{\tau=1}^{m}\chi_\tau+\omega\sum_{i=1}^{L}\alpha_i(\sum_{\tau=1}^{m}\xi_{i,\tau,0})+\omega\sum_{i=1}^{L}\beta_i(\sum_{\tau=1}^{m}\xi_{i,\tau,1})} \\
&= g_T^{\zeta}
\end{aligned}
$$

[0069] つまり、（Ｓ４０１）から（Ｓ４０７）において、復号装置３００は、数１４４に示すＤｅｃアルゴリズムを実行して、メッセージｍｓｇ’（＝ｍｓｇ）を生成する。

[数144]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)},\boldsymbol{k}_1^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$

$$\mathsf{ct}_{\Gamma} := (\Gamma,\boldsymbol{c}_0,\{\boldsymbol{c}_t\}_{(t,\vec{x}_t)\in\Gamma},c_{d+1})):$$

If $\mathbb{S} := (\mathcal{A},\mathcal{B},d(x),\ \rho)$ accepts $\Gamma := \{(t,\vec{x}_t)\}$,

then compute $\mathcal{I}_{(\rho,\Gamma)} \subseteq \{1,\ldots,L\},(\alpha_1,\ldots,\alpha_L)$,

$(\beta_1,\ldots,\beta_L)$ with $\alpha_i = 0 = \beta_i$ for all $i \notin \mathcal{I}_{(\rho,\Gamma)}$, and $(\kappa_1,\ldots,\kappa_m)$ such that

$\prod_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau} \mid (a_0(x)+\sum_{i=1}^{L}\alpha_i a_i(x))$,

and $\prod_{\tau=1}^{m} d_\tau(x)^{f\tau-\kappa_\tau} \mid (b_0(x)+\sum_{i=1}^{L}\beta_i b_i(x))$,

$$K_{\tau,0} := e(\boldsymbol{c}_0,\boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)})\cdot\prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$

$$\cdot\prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}\cdot\prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0,\boldsymbol{k}_0^{*(\tau,\kappa_\tau,1)})\cdot\prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$

$$\cdot\prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}\cdot\prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

where $\mathcal{I}_{(\rho,\Gamma),0} := \{i\in\mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\}$,

$\mathcal{I}_{(\rho,\Gamma),+} := \{i\in\mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t,\vec{v}_i)\}$ and

$\mathcal{I}_{(\rho,\Gamma),-} := \{i\in\mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t,\vec{v}_i)\}$.

return $msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1})$.

[0070] 以上のように、実施の形態２に係る暗号システム１０では、２次スパンプログラムを利用した関数型暗号方式を実現する。

２次スパンプログラムを利用することにより、関係Ｒとして表現できる範囲が広い。

[0071] 特に、実施の形態２に係る暗号システム１０では、目標多項式ｄ（ｘ）を因数分解した多項式$ｄ_{\tau}$（ｘ）$^{ｆ\tau}$毎に、多項式$ｄ_{\tau}$（ｘ）$^{\kappa}$で多項式$ａ_{ｉ}$（ｘ）を割った余りを設定した要素と、多項式$ｄ_{\tau}$（ｘ）$^{ｆ\tau-\kappa}$で多項式$ｂ_{ｉ}$（ｘ）を

割った余りを設定した要素とを、鍵要素$k^*_{0^{(\tau,\kappa,\iota)}}$，$k^*_{1^{(\tau,\kappa,\iota)}}$，．．．，$k^*_{L^{(\tau,\kappa,\iota)}}$とする。また、各鍵要素$k^*_{0^{(\tau,\kappa,\iota)}}$に、秘密情報$\pi$と秘密情報$\chi$とを分散させて設定する。そして、係数$\alpha$，$\beta$を用いて、鍵要素と暗号要素とのペアリング演算をすることにより、各鍵要素に設定された余りを０にし、秘密情報πを０にし、秘密情報χを１にすることにより、暗号文からセッション鍵$K_{\tau,0}$，$K_{\tau,1}$を抽出する。これにより、２次スパンプログラムを利用した関数型暗号方式を実現する。

[0072] なお、上記説明では、ＫＰ－ＦＥ方式について説明した。しかし、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズム、Ｄｅｃアルゴリズムをそれぞれ数１４５から数１４８に示すようにすることにより、ＣＰ－ＦＥ方式とすることも可能である。なお、Ｓｅｔｕｐアルゴリズムは、ＫＰ－ＦＥ方式とＣＰ－ＦＥ方式とで同じである。

[数145]

$$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \Gamma := \{(t,\vec{x}_t)\,|\,1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$\boldsymbol{k}_0^* := (\overbrace{\omega,\ 0,...,0,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\varphi}_0,}^{w_0}\ \overbrace{0,...,0,1}^{z_0})\,\mathbb{B}_0^*,$$

$$\boldsymbol{k}_t^* := (\overbrace{\omega\vec{x}_t,\ 0,...,0}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\varphi}_t,}^{w_t}\ \overbrace{0,...,0}^{z_t})\,\mathbb{B}_t^*,\ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$\text{return}\ \ \mathsf{sk}_\Gamma := (\Gamma,\ \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma}).$$

[数146]

$$\mathrm{Enc}\left(\mathrm{pk},\ msg,\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \ \kappa=0,\ldots,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x+\cdots+a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x+\cdots+b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (j=0,\ldots,\mu^{(\tau,\kappa,\iota)}-1),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1}\delta_j^{(\tau,\kappa,0)}\cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1}\delta_j^{(\tau,\kappa,1)}\cdot b_{0,j}^{(\tau,\kappa)},$$

[数147]

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{0,\ldots,0}^{w_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)},\ \zeta\chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0\ ,$$

for $i = 1,\ldots,L$,

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \ (i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\ (i = 1,\ldots,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

if $\rho(i) = (t,\vec{v}_i)$, $\quad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t}$,

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{0,\ldots,0}^{w_t},\ \overbrace{\vec{\eta}_i}^{z_t})\ \mathbb{B}_t\ ,$$

if $\rho(i) = \neg(t,\vec{v}_i)$, $\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t}$,

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{0,\ldots,0}^{w_t},\ \overbrace{\vec{\eta}_i}^{z_t})\ \mathbb{B}_t\ ,$$

if $\rho(i) = p_0$, $\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_0}$,

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{0,\ldots,0}^{w_0},\ \overbrace{\vec{\eta}_i}^{z_0})\ \mathbb{B}_0\ ,$$

$$c_{d+1} := g_T^{\zeta} msg,$$

return $\mathrm{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_0^{(\tau,\kappa,\iota)}, \boldsymbol{c}_1^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{c}_L^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1})$.

[数148]

$$\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\Gamma} := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma}),$$

$$\mathrm{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_0^{(\tau,\kappa,\iota)}, \boldsymbol{c}_1^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{c}_L^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1})):$$

If $\mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x), \rho)$ accepts $\Gamma := \{(t, \vec{x}_t)\}$,

then compute $\mathcal{I}_{(\rho,\Gamma)} \subseteq \{1,\ldots,L\}, (\alpha_1,\ldots,\alpha_L)$,

$(\beta_1,\ldots,\beta_L)$ with $\alpha_i = 0 = \beta_i$ for all $i \notin \mathcal{I}_{(\rho,\Gamma)}$, and $(\kappa_1,\ldots,\kappa_m)$ such that

$\prod_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x))$,

and $\prod_{\tau=1}^{m} d_\tau(x)^{f\tau-\kappa_\tau} \mid (b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x))$,

$$K_{\tau,0} := e(\boldsymbol{k}_0, \boldsymbol{c}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{k}_0, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$

$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{k}_0, \boldsymbol{c}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{k}_0, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$

$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{k}_t, \boldsymbol{c}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

where $\mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\}$,

$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t, \vec{v}_i)\}$ and

$\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t, \vec{v}_i)\}$.

return $msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1})$.

[0073] また、上記説明では、関数型暗号方式について説明した。しかし、Ｓｅｔｕｐアルゴリズム、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズム、Ｄｅｃアルゴリズムをそれぞれ数１４９から数１５３に示すようにすることにより、属性ベース暗号方式とすることも可能である。なお、属性ベース暗号方式の場合、Ｓｅｔｕｐアルゴリズムにおいて、n_tは$2mf_{max}k_{max}+2$である。

[数149]

$$\mathsf{Setup}(1^{\lambda}):$$

$$(\mathsf{param}, (\mathbb{B}_t, \mathbb{B}_t^*)_{t=0,\ldots,d}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^{\lambda})$$

$$\hat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}),$$

$$\hat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \boldsymbol{b}_{t,2}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}) \quad \text{for } t = 1,..,d,$$

$$\hat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \ldots, \boldsymbol{b}_{0,n_0}^*, \boldsymbol{b}_{0,n_0+u_0+1}^*, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^*, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^*),$$

$$\hat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,n_t+u_t+1}^*, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^*) \quad \text{for } t = 1,..,d,$$

$$\text{return } \mathsf{pk} := (1^{\lambda}, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \mathsf{param}), \quad \mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,\ldots,d}.$$

[数150]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \ \kappa=0,\ldots,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x+\cdots+a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x+\cdots+b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (j=0,\ldots,\mu^{(\tau,\kappa,\iota)}-1),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1}\delta_j^{(\tau,\kappa,0)}\cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1}\delta_j^{(\tau,\kappa,1)}\cdot b_{0,j}^{(\tau,\kappa)},$$

[数151]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0},\ \overbrace{0,\ldots,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^*,$$

for $i = 1,\ldots,L$,

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i = 1,\ldots,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

if $\rho(i) = (t, v_i)$, $\quad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} + \theta_i v_i,\ -\theta_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}_t^*,$$

if $\rho(i) = \neg(t, v_i)$, $\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} v_i,\ -s_i^{(\tau,\kappa,\iota)},\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\ \mathbb{B}_t^*,$$

if $\rho(i) = p_0$, $\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)},\ \vec{e}_0^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_i,}^{w_0}\ \overbrace{0,\ldots,0}^{w_0})\ \mathbb{B}_0^*,$$

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1})$.

[数152]

$$\mathsf{Enc}(\mathsf{pk},\ msg,\ \Gamma := \{(t,x_t)\,|\,1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},$$

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t} \text{ for } (t,x_t) \in \Gamma,$$

$$\boldsymbol{c}_0 := (\overbrace{\omega,\ 0,...,0,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...,0,}^{w_0}\ \overbrace{\vec{\varphi}_0,\ \zeta}^{z_0})\,\mathbb{B}_0\ ,$$

$$\boldsymbol{c}_t := (\overbrace{\omega(1,x_t),\ 0,...,0}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\varphi}_t}^{z_t})\,\mathbb{B}_t\ ,\ \text{for } (t,x_t) \in \Gamma,$$

$$c_{d+1} := g_T^{\zeta} msg,\ \ \mathsf{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1}),$$

return ct_Γ.

[数153]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)},\boldsymbol{k}_1^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$

$$\mathsf{ct}_\Gamma := (\Gamma,\boldsymbol{c}_0,\{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma},c_{d+1})):$$

If $\mathbb{S} := (\mathcal{A},\mathcal{B},d(x),\ \rho)$ accepts $\Gamma := \{(t,x_t)\}$,

then compute $\mathcal{I}_{(\rho,\Gamma)} \subseteq \{1,\ldots,L\},(\alpha_1,\ldots,\alpha_L)$,

$(\beta_1,\ldots,\beta_L)$ with $\alpha_i = 0 = \beta_i$ for all $i \notin \mathcal{I}_{(\rho,\Gamma)}$, and $(\kappa_1,\ldots,\kappa_m)$ such that

$\prod_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau} \mid (a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x))$,

and $\prod_{\tau=1}^{m} d_\tau(x)^{f\tau-\kappa_\tau} \mid (b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x))$,

$$K_{\tau,0} := e(\boldsymbol{c}_0,\boldsymbol{k}_0^{*(\tau,\kappa_\tau,0)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i}$$

$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,0)})^{\alpha_i/(v_i-x_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0,\boldsymbol{k}_0^{*(\tau,\kappa_\tau,1)}) \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),0}} e(\boldsymbol{c}_0,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i}$$

$$\cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),+}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i} \cdot \prod_{i\in\mathcal{I}_{(\rho,\Gamma),-}} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa_\tau,1)})^{\beta_i/(v_i-x_t)},$$

where $\mathcal{I}_{(\rho,\Gamma),0} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = p_0\}$,

$\mathcal{I}_{(\rho,\Gamma),+} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = (t,v_i)\}$ and

$\mathcal{I}_{(\rho,\Gamma),-} := \{i \in \mathcal{I}_{(\rho,\Gamma)} \mid \rho(i) = \neg(t,v_i)\}$.

return $msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1})$.

同様に、数１４５から数１４８に示すＣＰ－ＦＥ方式を属性ベース暗号方式に変更することも可能である。

[0074] また、上記説明では、N_0に$n_0+u_0+w_0+z_0$を設定し、N_tに$n_t+u_t+w_t+z_t$を設定した。ここで、例えば、$u_0=n_0$，$w_0=n_0$，$z_0=2$として、N_0に$n_0+n_0+n_0+2=3n_0+2$とし、$u_t=n_t$，$w_t=n_t$，$z_t=1$として、N_tに$n_t+n_t+n_t+1=3n_t+1$としてもよい。

[0075] 実施の形態３．

実施の形態３では、実施の形態２で説明した関数型暗号方式に比べ、基底の数が多くなる代わりに、各基底の次元数が少ない関数型暗号方式を説明する。

実施の形態３では、実施の形態２に係る暗号システム１０と異なる部分を中心に説明する。

[0076] 実施の形態３に係る鍵生成装置１００、暗号化装置２００、復号装置３００の構成は、図５～図７に示す実施の形態２に係る鍵生成装置１００、暗号化装置２００、復号装置３００の構成と同じである。

実施の形態３に係るＤｅｃアルゴリズムの処理については、実施の形態２に係るＤｅｃアルゴリズムの処理と同じであるため、ここでは、実施の形態３に係るＳｅｔｕｐアルゴリズム、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズムの処理について説明する。

実施の形態３に係るＳｅｔｕｐアルゴリズム、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズムの処理の流れは、図８～図１０に示す実施の形態２に係るＳｅｔｕｐアルゴリズム、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズムの処理の流れと同じである。

[0077] 図８に基づき、Ｓｅｔｕｐアルゴリズムの処理について説明する。

（Ｓ１０１：正規直交基底生成ステップ）

（１）～（３）の処理は、実施の形態２と同じである。

（４）マスター鍵生成部１１０は、N_0に$n_0+u_0+w_0+z_0$を設定し、ｔ＝１，．．．，ｄ（ｄは１以上の整数）の各整数ｔについて、N_tに$n_t+u_t+w_t+z_t$を設定する。ここで、n_0は１であり、n_tはｎである。ｎは１以上の整数であり、u_0，w_0，z_0，u_t，w_t，z_tはそれぞれ０以上の整数である。

続いて、マスター鍵生成部１１０は、τ＝１，．．．，ｍ、κ＝０，．．．，f_τ、ι＝０，１、ｔ＝０，．．．，ｄの各整数τ、κ、ι、ｔについて（５）から（９）までの処理を実行する。

（５）の処理は、実施の形態２と同じである。

（６）マスター鍵生成部１１０は、実施の形態２と同様に、線形変換$X_t^{(\tau,\kappa,\iota)}:=(\chi_{t,i,j}^{(\tau,\kappa,\iota)})_{i,j}$をランダムに生成する。

（７）マスター鍵生成部１１０は、実施の形態２と同様に、$X^*_t{}^{(\tau,\kappa,\iota)}:=(\nu_{t,i,j}^{(\tau,\kappa,\iota)})_{i,j}:=\phi\cdot(X_t^{(\tau,\kappa,\iota)\mathrm{T}})^{-1}$を生成する。

（８）マスター鍵生成部１１０は、実施の形態２と同様に、（６）で生成した線形変換$X_t^{(\tau,\kappa,\iota)}$に基づき、（５）で生成した標準基底$A_t$から基底$B_t^{(\tau,\kappa,\iota)}$を生成する。

（９）マスター鍵生成部１１０は、実施の形態２と同様に、（７）で生成した線形変換$X^*_t{}^{(\tau,\kappa,\iota)}$に基づき、（５）で生成した標準基底$A_t$から基底$B^*_t{}^{(\tau,\kappa,\iota)}$を生成する。

（１０）の処理は、実施の形態２と同じである。

[0078] （Ｓ１０２：公開パラメータ生成ステップ）

マスター鍵生成部１１０は、処理装置により、（Ｓ１０１）で生成した基底$B_0^{(\tau,\kappa,\iota)}$の部分基底$\hat{B}_0^{(\tau,\kappa,\iota)}$と、基底$B_t^{(\tau,\kappa,\iota)}$の部分基底$\hat{B}_t^{(\tau,\kappa,\iota)}$とを数１５４に示すように生成する。

[数154]

$$\hat{\mathbb{B}}_0^{(\tau,\kappa,\iota)}:=(\boldsymbol{b}_{0,1}^{(\tau,\kappa,\iota)},\boldsymbol{b}_{0,n_0+u_0+w_0+1}^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{(\tau,\kappa,\iota)}),$$
$$\hat{\mathbb{B}}_t^{(\tau,\kappa,\iota)}:=(\boldsymbol{b}_{t,1}^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{t,n}^{(\tau,\kappa,\iota)},\boldsymbol{b}_{t,n_t+u_t+w_t+1}^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{t,n_t+u_t+w_t+z_t}^{(\tau,\kappa,\iota)})$$
$$\text{for } t=1,..,d$$

マスター鍵生成部１１０は、生成した部分基底$\hat{B}_0^{(\tau,\kappa,\iota)}$及び部分基底$\hat{B}_t^{(\tau,\kappa,\iota)}$と、（Ｓ１０１）で入力されたセキュリティパラメータλと、（Ｓ１０１）で生成したｐａｒａｍとを合わせて、公開パラメータｐｋとする。

[0079] （Ｓ１０３：マスター鍵生成ステップ）

マスター鍵生成部１１０は、処理装置により、（Ｓ１０１）で生成した基底$B^*_0{}^{(\tau,\kappa,\iota)}$の部分基底$\hat{B}^*_0{}^{(\tau,\kappa,\iota)}$と、基底$B^*_t{}^{(\tau,\kappa,\iota)}$の部分基底

Ｂ＾＊$_{t}^{(\tau,\kappa,\iota)}$とを数１５５に示すように生成する。

[数155]

$$\hat{\mathbb{B}}_0^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{0,n_0}^{*(\tau,\kappa,\iota)},$$
$$\boldsymbol{b}_{0,n_0+u_0+1}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{0,n_0+u_0+w_0}^{*(\tau,\kappa,\iota)},\boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{*(\tau,\kappa,\iota)}),$$
$$\hat{\mathbb{B}}_t^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{t,n_t}^{*(\tau,\kappa,\iota)},\boldsymbol{b}_{t,n_t+u_t+1}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{b}_{t,n_t+u_t+w_t}^{*(\tau,\kappa,\iota)})$$
$$\text{for } t=1,..,d$$

マスター鍵生成部１１０は、生成した部分基底Ｂ＾＊$_{0}^{(\tau,\kappa,\iota)}$と部分基底Ｂ＾＊$_{t}^{(\tau,\kappa,\iota)}$とをマスター鍵ｓｋとする。

[0080] （Ｓ１０４）の処理は、実施の形態２と同じである。

[0081] つまり、（Ｓ１０１）から（Ｓ１０３）において、鍵生成装置１００は、数１５６に示すＳｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター鍵ｓｋとを生成する。そして、（Ｓ１０４）で、鍵生成装置１００は、生成した公開パラメータｐｋとマスター鍵ｓｋとを記憶装置に記憶する。

[数156]

$$\mathsf{Setup}(1^{\lambda}):$$

$$(\mathsf{param}, (\mathbb{B}_t^{(\tau,\kappa,\iota)}, \mathbb{B}_t^{*(\tau,\kappa,\iota)})_{t=0,\ldots,d;\ \tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau;\ \iota=0,1}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^{\lambda}),$$

$$\text{for } \tau=1,\ldots,m,\quad \kappa=0,\ldots,f_\tau,\quad \iota=0,1,$$

$$\hat{\mathbb{B}}_0^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}^{(\tau,\kappa,\iota)})$$

$$\text{for } t=1,..,d,$$

$$\hat{\mathbb{B}}_0^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{*(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t}^{*(\tau,\kappa,\iota)})$$

$$\text{for } t=1,..,d,$$

$$\text{return } \mathsf{pk} := (1^{\lambda}, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \mathsf{param}), \qquad \mathsf{sk} := \{\hat{\mathbb{B}}_t^{*}\}_{t=0,\ldots,d}.$$

[0082] 図９に基づき、ＫｅｙＧｅｎアルゴリズムの処理について説明する。

（Ｓ２０１）から（Ｓ２０４）までと、（Ｓ２０６）との処理は、実施の形態２と同じである。

[0083] （Ｓ２０５：鍵要素生成ステップ）

鍵要素生成部１４２は、処理装置により、τ＝１，．．．，ｍの各整数τと、κ＝０，．．．，ｆ$_\tau$の各整数κと、ι＝０，１の各整数ιとについて、復号鍵ｓｋ$_S$の要素ｋ*$_0^{(\tau,\kappa,\iota)}$を数１５７に示すように生成する。

[数157]

$$\vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{U} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}, \ldots}^{n_0}, \overbrace{0,\ldots,0}^{u_0}, \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0}, \overbrace{0,\ldots,0, \chi_{\tau,\kappa,\iota}}^{z_0}) \mathbb{B}_0^{*(\tau,\kappa,\iota)}$$

鍵要素生成部１４２は、処理装置により、τ＝１，．．．．，ｍの各整数τと、κ＝０，．．．．，ｆ$_{\tau}$の各整数κと、ι＝０，１の各整数ιと、ｉ＝１，．．．．，Ｌの各整数ｉとについて、復号鍵ｓｋ$_{S}$の要素ｋ＊$_{i}^{(\tau,\kappa,\iota)}$を数１５８に示すように生成する。

[数158]

$$\text{if } \rho(i)=(t,\vec{v}_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1+\theta_i\vec{v}_i}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

$$\text{if } \rho(i)=\neg(t,\vec{v}_i),\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

$$\text{if } \rho(i)=p_0,\qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_i}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^{*(\tau,\kappa,\iota)}$$

[0084] つまり、（Ｓ２０１）から（Ｓ２０５）において、鍵生成装置１００は、数１５９から数１６０に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵ｓｋ$_{S}$を生成する。そして、（Ｓ２０６）で、鍵生成装置１００は、生成した復号鍵ｓｋ$_{S}$を復号装置３００へ配布する。

[数159]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \ \kappa=0,\ldots,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x + \cdots + a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x + \cdots + b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)} x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \left(j=0,\ldots,\mu^{(\tau,\kappa,\iota)}-1\right),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{0,j}^{(\tau,\kappa)},$$

[数160]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0}, \overbrace{0,...,0}^{u_0}, \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0}, \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\, \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

for $i = 1,...,L$,

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i = 1,...,L;\ \tau = 1,...,m-1; \iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i = 1,...,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

if $\rho(i) = (t, \vec{v}_i)$, $\theta_i \xleftarrow{\cup} \mathbb{F}_q$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i \vec{v}_i}^{n_t}, \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t})\, \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

if $\rho(i) = \neg(t, \vec{v}_i)$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i}^{n_t}, \overbrace{0,...,0,}^{u_t} \overbrace{\vec{\eta}_i,}^{w_t} \overbrace{0,...,0}^{z_t})\, \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

if $\rho(i) = p_0$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}}^{n_0}, \overbrace{0,...,0,}^{u_0} \overbrace{\vec{\eta}_i,}^{w_0} \overbrace{0,...,0}^{z_0})\, \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1})$.

[0085] 図１０に基づき、Ｅｎｃアルゴリズムの処理について説明する。

（Ｓ３０１）から（Ｓ３０２）までと、（Ｓ３０４）との処理は、実施の形態２と同じである。

[0086] （Ｓ３０３：暗号要素生成ステップ）

暗号化データ生成部２３０は、処理装置により、暗号文ｃｔ┌の要素ｃ$_0^{(\tau,\kappa,\iota)}$を数１６１に示すように生成する。

[数161]

$$\omega,\zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$
$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},$$
$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{\omega,}^{n_0}\overbrace{0,...,0,}^{u_0}\overbrace{0,...,0,}^{w_0}\overbrace{\vec{\varphi}_0,\zeta}^{z_0})_{\mathbb{B}_0^{(\tau,\kappa,\iota)}}$$

暗号化データ生成部２３０は、処理装置により、属性情報Γに含まれる各整数ｔについて、暗号文ｃｔ$_{\Gamma}$の要素ｃ$_{t}$$^{(\tau,\kappa,\iota)}$を数１６２に示すように生成する。

[数162]

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t} \text{ for } (t,\vec{x}_t)\in\Gamma,$$
$$\boldsymbol{c}_t^{(\tau,\kappa,\iota)} := (\overbrace{\omega\vec{x}_t,}^{n_t}\overbrace{0,...,0,}^{u_t}\overbrace{0,...,0,}^{w_t}\overbrace{\vec{\varphi}_t}^{z_t})_{\mathbb{B}_t^{(\tau,\kappa,\iota)}}$$

暗号化データ生成部２３０は、処理装置により、暗号文ｃｔ$_{\Gamma}$の要素ｃ$_{d+1}$を数１６３に示すように生成する。

[数163]

$$c_{d+1} := g_T^{\zeta} msg$$

[0087] つまり、（Ｓ３０１）から（Ｓ３０３）において、暗号化装置２００は、数１６４に示すＥｎｃアルゴリズムを実行して、暗号文ｃｔ$_{\Gamma}$を生成する。そして、（Ｓ３０４）で、暗号化装置２００は生成した暗号文ｃｔ$_{\Gamma}$を復号装置３００へ送信する。

[数164]

$$\mathrm{Enc}(\mathrm{pk},\ msg,\ \Gamma := \{(t,\vec{x}_t)\,|\,1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},$$

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t} \ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{\omega,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...,0,}^{w_0}\ \overbrace{\vec{\varphi}_0,\ \zeta}^{z_0})\,\mathbb{B}_0^{(\tau,\kappa,\iota)},$$

$$\boldsymbol{c}_t^{(\tau,\kappa,\iota)} := (\overbrace{\omega\vec{x}_t,}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\varphi}_t}^{z_t})\,\mathbb{B}_t^{(\tau,\kappa,\iota)},\ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$c_{d+1} := g_T^{\zeta} msg,$$

$$\text{return}\ \ \mathrm{ct}_\Gamma := (\Gamma, \boldsymbol{c}_0, \{\boldsymbol{c}_t\}_{(t,\vec{x}_t)\in\Gamma}, c_{d+1}).$$

[0088] 以上のように、実施の形態３に係る暗号システム１０は、実施の形態２で説明した関数型暗号方式に比べ、基底の数が多くなる代わりに、各基底の次元数が少ない関数型暗号方式を実現する。

[0089] なお、上記説明では、ＫＰ－ＦＥ方式について説明した。しかし、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズムをそれぞれ数１６５から数１６７に示すようにすることにより、ＣＰ－ＦＥ方式とすることも可能である。なお、Ｓｅｔｕｐアルゴリズムは、ＫＰ－ＦＥ方式とＣＰ－ＦＥ方式とで同じである。また、Ｄｅｃアルゴリズムは、数１４８に示すＤｅｃアルゴリズムと同じである。

[数165]

$$\mathsf{KeyGen}(\mathsf{pk},\ \mathsf{sk},\ \Gamma := \{(t,\vec{x}_t) \mid 1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{\omega,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\varphi}_0,}^{w_0}\ \overbrace{0,...,0,1}^{z_0})\,\mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

$$\boldsymbol{k}_t^{*(\tau,\kappa,\iota)} := (\overbrace{\omega\vec{x}_t,}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\varphi}_t,}^{w_t}\ \overbrace{0,...,0}^{z_t})\,\mathbb{B}_t^{*(\tau,\kappa,\iota)},\ \text{for}\ (t,\vec{x}_t) \in \Gamma$$

$$\text{return}\ \ \mathsf{sk}_\Gamma := (\Gamma,\ \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma}).$$

[数166]

$$\mathrm{Enc}\left(\mathrm{pk},\ msg,\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \kappa=0,\ldots,f_\tau,\ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x+\cdots+a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x+\cdots+b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (j=0,\ldots,\mu^{(\tau,\kappa,\iota)}-1),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1}\delta_j^{(\tau,\kappa,0)}\cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1}\delta_j^{(\tau,\kappa,1)}\cdot b_{0,j}^{(\tau,\kappa)},$$

[数167]

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0}, \overbrace{0,\ldots,0}^{u_0}, \overbrace{0,\ldots,0}^{w_0}, \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}, \zeta\chi_{\tau,\kappa,\iota}}^{z_0})\, \mathbb{B}_0^{(\tau,\kappa,\iota)},$$

for $i = 1,\ldots,L,$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i = 1,\ldots,L;\ \tau = 1,\ldots,m-1; \iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i = 1,\ldots,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

if $\rho(i) = (t, \vec{v}_i)$, $\theta_i \xleftarrow{\cup} \mathbb{F}_q$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t}$,

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{e}_1 + \theta_i\vec{v}_i}^{n_t}, \overbrace{0,\ldots,0}^{u_t}, \overbrace{0,\ldots,0}^{w_t}, \overbrace{\vec{\eta}_i}^{z_t})\, \mathbb{B}_t^{(\tau,\kappa,\iota)},$$

if $\rho(i) = \neg(t, \vec{v}_i)$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t}$,

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}\vec{v}_i}^{n_t}, \overbrace{0,\ldots,0}^{u_t}, \overbrace{0,\ldots,0}^{w_t}, \overbrace{\vec{\eta}_i}^{z_t})\, \mathbb{B}_t^{(\tau,\kappa,\iota)},$$

if $\rho(i) = p_0$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_0}$,

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}}^{n_0}, \overbrace{0,\ldots,0}^{u_0}, \overbrace{0,\ldots,0}^{w_0}, \overbrace{\vec{\eta}_i}^{z_0})\, \mathbb{B}_0^{(\tau,\kappa,\iota)},$$

$$c_{d+1} := g_T^{\zeta} msg,$$

return $\mathrm{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_0^{(\tau,\kappa,\iota)}, \boldsymbol{c}_1^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{c}_L^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1})$.

[0090] また、上記説明では、関数型暗号方式について説明した。しかし、Ｓｅｔｕｐアルゴリズム、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズムをそれぞれ数１６８から数１７１に示すようにすることにより、属性ベース暗号方式とすることも可能である。なお、属性ベース暗号方式の場合、Ｓｅｔｕｐアルゴリズムにおいて、n_tは２である。Ｄｅｃアルゴリズムは、数１５３に示すＤｅｃアルゴリズムと同じである。

[数168]

$$\mathsf{Setup}(1^{\lambda}):$$

$$(\mathsf{param}, (\mathbb{B}_t^{(\tau,\kappa,\iota)}, \mathbb{B}_t^{*(\tau,\kappa,\iota)})_{t=0,\ldots,d;\ \tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau;\ \iota=0,1}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^{\lambda}),$$

$$\text{for } \tau=1,\ldots,m,\quad \kappa=0,\ldots,f_\tau,\quad \iota=0,1,$$

$$\hat{\mathbb{B}}_0^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,n_0+u_0+w_0+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,n_0+u_0+w_0+z_0}^{(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,2}^{(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,n_t+u_t+w_t+1}^{(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,n_t+u_t+w_t+z_t}^{(\tau,\kappa,\iota)})$$

$$\text{for } t=1,..,d,$$

$$\hat{\mathbb{B}}_0^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{0,1}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,1+u_0+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{0,1+u_0+w_0}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{0,1+u_0+w_0+z_0}^{*(\tau,\kappa,\iota)}),$$

$$\hat{\mathbb{B}}_t^{*(\tau,\kappa,\iota)} := (\boldsymbol{b}_{t,1}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,2}^{*(\tau,\kappa,\iota)}, \boldsymbol{b}_{t,2+u_t+1}^{*(\tau,\kappa,\iota)}, \ldots, \boldsymbol{b}_{t,2+u_t+w_t}^{*(\tau,\kappa,\iota)})$$

$$\text{for } t=1,..,d,$$

$$\text{return } \mathsf{pk} := (1^{\lambda}, \{\hat{\mathbb{B}}_t\}_{t=0,\ldots,d}, \mathsf{param}),\qquad \mathsf{sk} := \{\hat{\mathbb{B}}_t^{*}\}_{t=0,\ldots,d}.$$

[数169]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \ \kappa=0,\ldots,f_\tau,\ \ \iota=0,1,$

$$\mu^{(\tau,\kappa,0)} := \deg(d_\tau(x)^\kappa),\ \ \mu^{(\tau,\kappa,1)} := \deg(d_\tau(x)^{f_\tau-\kappa}),\ \ (\kappa=0,\ldots,f_\tau),$$

$$a_{i,0}^{(\tau,\kappa)} + a_{i,1}^{(\tau,\kappa)}x+\cdots+a_{i,\mu^{(\tau,\kappa,0)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,0)}-1} := a_i(x) \bmod\ d_\tau(x)^\kappa,$$

$$b_{i,0}^{(\tau,\kappa)} + b_{i,1}^{(\tau,\kappa)}x+\cdots+b_{i,\mu^{(\tau,\kappa,1)}-1}^{(\tau,\kappa)}x^{\mu^{(\tau,\kappa,1)}-1} := b_i(x) \bmod\ d_\tau(x)^{f_\tau-\kappa},$$

$$\delta_j^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (j=0,\ldots,\mu^{(\tau,\kappa,\iota)}-1),\ \ \vec{\eta}_0^{(\tau,\kappa,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$s_0^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1}\delta_j^{(\tau,\kappa,0)}\cdot a_{0,j}^{(\tau,\kappa)},$$

$$s_0^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1}\delta_j^{(\tau,\kappa,1)}\cdot b_{0,j}^{(\tau,\kappa)},$$

[数170]

$$\boldsymbol{k}_0^{*(\tau,\kappa,\iota)} := (\overbrace{s_0^{(\tau,\kappa,\iota)} + \pi_{\tau,\kappa,\iota}}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_0^{(\tau,\kappa,\iota)}}^{w_0},\ \overbrace{0,...,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\ \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

for $i = 1,...,L$,

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i = 1,...,L;\ \tau = 1,...,m-1; \iota = 0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i = 1,...,L;\ \iota = 0,1),$$

$$s_i^{(\tau,\kappa,0)} := \sum_{j=0}^{\mu^{(\tau,\kappa,0)}-1} \delta_j^{(\tau,\kappa,0)} \cdot a_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,0},$$

$$s_i^{(\tau,\kappa,1)} := \sum_{j=0}^{\mu^{(\tau,\kappa,1)}-1} \delta_j^{(\tau,\kappa,1)} \cdot b_{i,j}^{(\tau,\kappa)} + \xi_{i,\tau,1},$$

if $\rho(i) = (t, v_i)$, $\theta_i \xleftarrow{\cup} \mathbb{F}_q$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} + \theta_i v_i,\ -\theta_i}^{n_t},\ \overbrace{0,...,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

if $\rho(i) = \neg(t, v_i)$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)} v_i,\ -s_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,...,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,...,0}^{z_t})\ \mathbb{B}_t^{*(\tau,\kappa,\iota)},$$

if $\rho(i) = p_0$, $\vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_0}$,

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{s_i^{(\tau,\kappa,\iota)}}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_i}^{w_0},\ \overbrace{0,...,0}^{w_0})\ \mathbb{B}_0^{*(\tau,\kappa,\iota)},$$

return $\mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_0^{*(\tau,\kappa,\iota)}, \boldsymbol{k}_1^{*(\tau,\kappa,\iota)}, ..., \boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,...,m;\kappa=0,...,f_\tau;\iota=0,1})$.

[数171]

$$\mathrm{Enc}(\mathrm{pk}, msg, \Gamma := \{(t,x_t) \mid 1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0-1},$$

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t} \text{ for } (t,x_t) \in \Gamma,$$

$$\boldsymbol{c}_0^{(\tau,\kappa,\iota)} := (\overbrace{\omega,\ 0,...,0,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{0,...,0,}^{w_0}\ \overbrace{\vec{\varphi}_0,\ \zeta}^{z_0})\ \mathbb{B}_0^{(\tau,\kappa,\iota)},$$

$$\boldsymbol{c}_t^{(\tau,\kappa,\iota)} := (\overbrace{\omega(1,x_t),\ 0,...,0}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{0,...,0,}^{w_t}\ \overbrace{\vec{\varphi}_t}^{z_t})\ \mathbb{B}_t^{(\tau,\kappa,\iota)},\ \text{for } (t,x_t) \in \Gamma,$$

$$c_{d+1} := g_T^{\zeta} msg,$$

$$\text{return } \mathrm{ct}_\Gamma := (\Gamma, c_0, \{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma}, c_{d+1}).$$

同様に、数１６５から数１６７に示すＣＰ－ＦＥ方式を属性ベース暗号方式に変更することも可能である。

[0091] また、上記説明では、N_0に$n_0+u_0+w_0+z_0$を設定し、N_tに$n_t+u_t+w_t+z_t$を設定した。ここで、例えば、$u_0=n_0$，$w_0=n_0$，$z_0=2$として、N_0に$n_0+n_0+n_0+2=3n_0+2$（$n_0=1$のため、$N_0=5$）とし、$u_t=n_t$，$w_t=n_t$，$z_t=1$として、N_tに$n_t+n_t+n_t+1=3n_t+1$としてもよい。

[0092] 実施の形態４．

実施の形態２，３では、目標多項式ｄ（ｘ）を因数分解した多項式$d_\tau(x)^{f_\tau}$毎に、多項式$d_\tau(x)^{\kappa}$で多項式$a_i(x)$を割った余りを設定した要素と、多項式$d_\tau(x)^{f_\tau-\kappa}$で多項式$b_i(x)$を割った余りを設定した要素とを、鍵要素とした。

実施の形態４では、目標多項式ｄ（ｘ）を因数分解した多項式$d_\tau(x)^{f_\tau}$毎に、多項式$d_\tau(x)^{\kappa}$に乱数値γを代入した要素と、多項式$d_\tau(x)^{f_\tau-\kappa}$に乱数値$\gamma$を代入した要素とを、鍵要素とする。

[0093] 実施の形態４に係る鍵生成装置１００、暗号化装置２００、復号装置３００の構成は、図５～図７に示す実施の形態２に係る鍵生成装置１００、暗号化装置２００、復号装置３００の構成と同じである。

実施の形態４に係るＳｅｔｕｐアルゴリズム、Ｅｎｃアルゴリズムは、実施の形態２に係るＳｅｔｕｐアルゴリズム、Ｅｎｃアルゴリズムと同じである。

実施の形態４に係るＤｅｃアルゴリズムの処理の流れは、図１１に示す実施の形態２に係るＤｅｃアルゴリズムの処理の流れと同じである。

図１２は、実施の形態４に係るＫｅｙＧｅｎアルゴリズムの処理を示すフローチャートである。

[0094] 図１２に基づき、ＫｅｙＧｅｎアルゴリズムの処理について説明する。

（Ｓ５０１）から（Ｓ５０３）までの処理は、図９に示す（Ｓ２０１）から（Ｓ２０３）までの処理と同じであり、（Ｓ５０５）の処理は、図９に示す（Ｓ２０６）との処理と同じである。

[0095] （Ｓ５０４：鍵要素生成ステップ）

鍵要素生成部１４２は、処理装置により、$\tau=1,\ldots,m$の各整数τと、$\kappa=0,\ldots,f_{\tau}$の各整数κと、$\iota=0,1$の各整数ιと、$j=1,\ldots,\mu+1$の各整数jとについて、復号鍵sk_Sの要素$k^{*}_{0,j}{}^{(\tau,\kappa,\iota)}$と要素$k^{*}_{0,\mu+1}{}^{(\tau,\kappa,\iota)}$とを数１７２に示すように生成する。

[数172]

$$\gamma \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\eta}_{0,0},\ldots,\vec{\eta}_{0,\mu+1} \xleftarrow{\cup} \mathbb{F}_q^{w_0},$$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)} := (\overbrace{\delta(\gamma^j \cdot d_\tau(\gamma)^\kappa,\ \vec{e}_{0,j}^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_{0,j},}^{w_0}\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)} := (\overbrace{\delta(\gamma^j \cdot d_\tau(\gamma) f_\tau^{-\kappa},\ \vec{e}_{0,j}^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_{0,j},}^{w_0}\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$s_0 := -a_0(\gamma) \text{ if } \iota = 0,\quad s_0 := -b_0(\gamma) \text{ if } \iota = 1,$$

$$\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_0 + \pi_{\tau,\kappa,\iota},\ \vec{e}_{0,\mu+1}^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{\vec{\eta}_{0,\mu+1},}^{w_0}\ \overbrace{0,\ldots,0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0^*$$

鍵要素生成部１４２は、処理装置により、τ＝１，．．．．，ｍの各整数τと、κ＝０，．．．．，ｆ$_\tau$の各整数κと、ι＝０，１の各整数ιと、ｉ＝１，．．．．，Ｌの各整数ｉとについて、復号鍵ｓｋ$_S$の要素ｋ*$_i^{(\tau,\kappa,\iota)}$を数１７３に示すように生成する。

[数173]

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q\ \left(i = 1,\ldots,L;\ \tau = 1,\ldots,m-1;\iota = 0,1\right),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota}\left(i = 1,\ldots,L;\ \iota = 0,1\right),$$

$$s_i := -a_i(\gamma) + \xi_{i,\tau,0} \text{ if } \iota = 0,\qquad s_i := -b_i(\gamma) + \xi_{i,\tau,1} \text{ if } \iota = 1,$$

$$\text{if } \rho(i) = (t,\vec{v}_i),\qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q,\quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i\vec{e}_1 + \theta_i\vec{v}_i),\ \vec{e}_i^{(\tau,\kappa,\iota)},}^{n_t}\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{if } \rho(i) = \neg(t,\vec{v}_i),\qquad \vec{\eta}_1 \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta s_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)},}^{n_t}\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{\vec{\eta}_i,}^{w_t}\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*$$

ここで、$\vec{e}_{0,j}^{(\tau,\kappa,\iota)}$（ｊ＝１，．．．，$\mu+1$）は、１つの基底ベクトルの係数として１が設定され、他の基底ベクトルの係数として０が設定された２ｍｆ$_{max}$次元のベクトルであって、係数として１が設定される基底ベクトルが（τ，κ，ι）毎に異なるベクトルである。

[0096] つまり、（Ｓ５０１）から（Ｓ５０４）において、鍵生成装置１００は、数１７４から数１７５に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵ｓｋ$_S$を生成する。そして、（Ｓ５０５）で、鍵生成装置１００は、生成した復号鍵ｓｋ$_S$を復号装置３００へ配布する。

[数174]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\quad \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\quad \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\text{for } \tau=1,\ldots,m,\ \kappa=0,\ldots,f_\tau,\ \iota=0,1,$$

$$\gamma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_{0,0},\ldots,\vec{\eta}_{0,\mu+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$\text{for } j=0,\ldots,\mu,$$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^\kappa,\ \vec{e}_{0,j}^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^{f_\tau-\kappa},\ \vec{e}_{0,j}^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,\ldots,0}^{z_0})\,\mathbb{B}_0^*,$$

$$s_0 := -a_0(\gamma)\ \text{ if }\ \iota=0,\quad s_0 := -b_0(\gamma)\ \text{ if }\ \iota=1,$$

$$\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_0+\pi_{\tau,\kappa,\iota},\ \vec{e}_{0,\mu+1}^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,\ldots,0}^{u_0},\ \overbrace{\vec{\eta}_{0,\mu+1}}^{w_0},\ \overbrace{0,\ldots0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0^*,$$

[数175]

$$\text{for } i=1,\ldots,L,$$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i=1,\ldots,L;\ \tau=1,\ldots,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i=1,\ldots,L;\ \iota=0,1),$$

$$s_i := -a_i(\gamma)+\xi_{i,\tau,0} \ \text{ if } \iota=0, \qquad s_i := -b_i(\gamma)+\xi_{i,\tau,1} \ \text{ if } \iota=1,$$

$$\text{if } \rho(i)=(t,\vec{v}_i), \qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q, \quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i\vec{e}_1+\theta_i\vec{v}_i),\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{if } \rho(i)=\neg(t,\vec{v}_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta s_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{return } \mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},\ \boldsymbol{k}_1^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}).$$

[0097] 図１１に基づき、Ｄｅｃアルゴリズムの処理について説明する。

（Ｓ４０１）から（Ｓ４０４）までの処理は、実施の形態２と同じである。

[0098] （Ｓ４０５：係数計算ステップ）

補完係数計算部３３０の係数計算部３３２は、処理装置により、数１７６となる係数（α_1，．．．，α_L）と、係数（β_1，．．．，β_L）と、次数κとを計算する。

[数176]

$$h_{\tau,\kappa,0}(x)\cdot d_\tau(x)^\kappa = a_0(x)+\sum_{i=1}^{L}\alpha_i a_i(x), \ \text{and}$$

$$h_{\tau,\kappa,1}(x)\cdot d_\tau(x)^{f_\tau-\kappa} = b_0(x)+\sum_{i=1}^{L}\beta_i b_i(x)$$

ここで、$I_{(\rho,\Gamma)}$に含まれない全てのｉについては、$\alpha_i=0=\beta_i$である。また、$\tau=1,\ldots,m$及び$\iota=0,1$の全ての整数τ，ιについて$h_{\tau,\kappa,\iota}(x):=h_{\tau,\kappa,\iota,0}+h_{\tau,\kappa,\iota,1}x+\cdots+h_{\tau,\kappa,\iota,\mu}x^{\mu}$である。

[0099] （Ｓ４０６：ペアリング演算ステップ）

復号部３４０のペアリング演算部３４１は、処理装置により、数１７７を計算して、セッション鍵$K_{\tau,0}$，$K_{\tau,1}$を生成する。

[数177]

$$K_{\tau,0}:=e(\boldsymbol{c}_0,\sum_{j=0}^{\mu}h_{\tau,\kappa,0,j}\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)})\cdot e(\boldsymbol{c}_0,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)})\cdot \prod_{i\in I_\delta,+}e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i}\cdot\prod_{i\in I_\delta,-}e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1}:=e(\boldsymbol{c}_0,\sum_{j=0}^{\mu}h_{\tau,\kappa,1,j}\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)})\cdot e(\boldsymbol{c}_0,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,1)})\cdot \prod_{i\in I_\delta,+}e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i}\cdot\prod_{i\in I_\delta,-}e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

where $I_{\delta,+}:=\{i\in I_\delta\mid\rho(i)=(t,\vec{v}_i)\}$ and $I_{\delta,-}:=\{i\in I_\delta\mid\rho(i)=\neg(t,\vec{v}_i)\}$

[0100] （Ｓ４０７：メッセージ計算ステップ）

メッセージ計算部３４２は、処理装置により、数１７８を計算して、メッセージｍｓｇ’（＝ｍｓｇ）を生成する。

[数178]

$$msg':=c_{d+1}/(\prod_{\tau=1}^{m}K_{\tau,0}K_{\tau,1})$$

なお、数１７９に示すように、数１７７を計算することによりg_T^{ζ}が得られる。そのため、数１７８を計算することにより、メッセージｍｓｇ’（＝ｍｓｇ）を得られる。

[数179]

$$K_{\tau,0} := e(\boldsymbol{c}_0, \sum_{j=0}^{\mu} h_{\tau,\kappa,0,j} \boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)}) \cdot e(\boldsymbol{c}_0, \boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)}) \cdot$$

$$\prod_{i \in I_\delta,+} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i} \cdot \prod_{i \in I_\delta,-} e(\boldsymbol{c}_t, \boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i/(\vec{v}_i \cdot \vec{x}_t)}$$

$$= g_T^{\delta\omega\left(\sum_{j=0}^{\mu} h_{\tau,\kappa,0,j} \gamma^j \cdot d_\tau(\gamma)^\kappa\right)} \cdot g_T^{\delta\omega\left(-a_0(\gamma)+\pi_{\tau,\kappa,0}\right)+\zeta\chi_{\tau,\kappa,0}}$$

$$\cdot g_T^{\delta\omega\sum_{i=1}^{L}\left(-\alpha_i a_i(\gamma)+\alpha_i \xi_{i,\tau,0}\right)}$$

$$= g_T^{\delta\omega h_{\tau,\kappa,0}(\gamma) \cdot d_\tau(\gamma)^\kappa} \cdot g_T^{-\delta\omega\left(a_0(\gamma)+\sum_{i=1}^{L}\alpha_i a_i(\gamma)\right)}$$

$$\cdot g_T^{\delta\omega\pi_{\tau,\kappa,0}+\zeta\chi_{\tau,\kappa,0}+\sum_{i=1}^{L}\alpha_i \xi_{i,\tau,0}}$$

$$= g_T^{\delta\omega\pi_{\tau,\kappa,0}+\zeta\chi_{\tau,\kappa,0}+\sum_{i=1}^{L}\alpha_i \xi_{i,\tau,0}}$$

$$K_{\tau,1} = g_T^{\delta\omega\pi_{\tau,\kappa,1}+\zeta\chi_{\tau,\kappa,1}+\sum_{i=1}^{L}\beta_i \xi_{i,\tau,1}}$$

$$\prod_{\tau=1}^{m} K_{\tau,0} K_{\tau,1} = g_T^{\sum_{\tau=1}^{m}(\delta\omega(\pi_{\tau,\kappa,0}+\pi_{\tau,\kappa,1})+\zeta(\chi_{\tau,\kappa,0}+\chi_{\tau,\kappa,1})+\sum_{i=1}^{L}(\alpha_i \xi_{i,\tau,0}+\beta_i \xi_{i,\tau,1}))}$$

$$= g_T^{\omega\sum_{\tau=1}^{m}\pi_\tau+\zeta\sum_{\tau=1}^{m}\chi_\tau+\omega\sum_{i=1}^{L}\alpha_i(\sum_{\tau=1}^{m}\xi_{i,\tau,0})+\omega\sum_{i=1}^{L}\beta_i(\sum_{\tau=1}^{m}\xi_{i,\tau,1})}$$

$$= g_T^{\zeta}$$

[0101] つまり、（Ｓ４０１）から（Ｓ４０７）において、復号装置３００は、数１８０に示すＤｅｃアルゴリズムを実行して、メッセージｍｓｇ’（＝ｍｓｇ）を生成する。

[数180]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},\ \boldsymbol{k}_{1}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{L}^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$

$$\mathsf{ct}_{\Gamma} := (\Gamma,\boldsymbol{c}_0,\{\boldsymbol{c}_t\}_{(t,\vec{x}_t)\in\Gamma},c_{d+1})):$$

if $\mathbb{S} := (\mathcal{A},\mathcal{B},d(x),\ \rho)$ accepts $\Gamma := \{(t,\vec{x}_t)\}$,

then compute $I_\delta \subseteq \{1,\ldots,L\},(\alpha_1,\ldots,\alpha_L),\ (\beta_1,\ldots,\beta_L)$ and

κ with $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}\ x + \cdots + h_{\tau,\kappa,\iota,\mu}\ x^{\mu}$

for all $\tau=1,\ldots,m$ and $\iota = 0,1$ such that

$h_{\tau,\kappa,0}(x)\cdot d_\tau(x)^{\kappa} = a_0(x) + \sum_{i=1}^{L}\alpha_i a_i(x)$, and

$h_{\tau,\kappa,1}(x)\cdot d_\tau(x)^{f_\tau-\kappa} = b_0(x) + \sum_{i=1}^{L}\beta_i b_i(x)$,

$$K_{\tau,0} := e(\boldsymbol{c}_0,\sum_{j=0}^{\mu}h_{\tau,\kappa,0,j}\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)})\cdot e(\boldsymbol{c}_0,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)})\cdot \prod_{i\in I_\delta,+} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i}\cdot\prod_{i\in I_\delta,-} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0,\sum_{j=0}^{\mu}h_{\tau,\kappa,1,j}\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)})\cdot e(\boldsymbol{c}_0,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,1)})\cdot \prod_{i\in I_\delta,+} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i}\cdot\prod_{i\in I_\delta,-} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

where $I_{\delta,+} := \{i\in I_\delta \mid \rho(i) = (t,\vec{v}_i)\}$ and $I_{\delta,-} := \{i\in I_\delta \mid \rho(i) = \neg(t,\vec{v}_i)\}$.

return $msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1})$.

[0102] 以上のように、実施の形態４に係る暗号システム１０は、多項式ｄ$_\tau$（ｘ）$^\kappa$に乱数値γを代入した要素と、多項式ｄ$_\tau$（ｘ）$^{f_\tau-\kappa}$に乱数値γを代入した要素とを、鍵要素として関数型暗号方式を実現する。

[0103] なお、上記説明では、ＫＰ－ＦＥ方式について説明した。しかし、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズム、Ｄｅｃアルゴリズムをそれぞれ数１８１から数１８４に示すようにすることにより、ＣＰ－ＦＥ方式とする

ことも可能である。なお、Ｓｅｔｕｐアルゴリズムは、ＫＰ－ＦＥ方式とＣＰ－ＦＥ方式とで同じである。

［数181］

$$\mathsf{KeyGen}(\mathsf{pk},\ \mathrm{sk},\ \Gamma := \{(t,\vec{x}_t)\,|\,1 \le t \le d\}):$$

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

$$\vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

$$\vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$\boldsymbol{k}_0^* := (\overbrace{\omega,\ 0,...,0,}^{n_0}\ \overbrace{0,...,0,}^{u_0}\ \overbrace{\vec{\varphi}_0,}^{w_0}\ \overbrace{0,...,0,1}^{z_0})\,\mathbb{B}_0^*\ ,$$

$$\boldsymbol{k}_t^* := (\overbrace{\omega\vec{x}_t,\ 0,...,0}^{n_t}\ \overbrace{0,...,0,}^{u_t}\ \overbrace{\vec{\varphi}_t,}^{w_t}\ \overbrace{0,...,0}^{z_t})\,\mathbb{B}_t^*\ ,\ \text{for}\ (t,\vec{x}_t) \in \Gamma,$$

$$\text{return}\ \ \mathsf{sk}_\Gamma := (\Gamma,\ \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma}).$$

[数182]

$$\mathrm{Enc}\left(\mathrm{pk},\ msg,\ \mathbb{S} := \left(\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho\right)\right):$$

$$\pi_\tau \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ (\tau=1,\ldots,m-1),\ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,\ldots,m;\ \kappa=0,\ldots,f_\tau),$$

for $\tau=1,\ldots,m,\ \kappa=0,\ldots,f_\tau,\ \iota=0,1,$

$$\gamma \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ \vec{\eta}_{0,0},\ldots,\vec{\eta}_{0,\mu} \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_0},\ \vec{\eta}_{0,\mu+1} \xleftarrow{\mathrm{U}} \mathbb{F}_q^{z_0-1}$$

for $j=0,\ldots,\mu,$

$$\boldsymbol{c}_{0,j}^{(\tau,\kappa,0)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^\kappa,\ \vec{e}_0^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{0,\ldots,0,}^{w_0}\ \overbrace{\vec{\eta}_{0,j}}^{z_0})\,\mathbb{B}_0,$$

$$\boldsymbol{c}_{0,j}^{(\tau,\kappa,1)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^{f_\tau-\kappa},\ \vec{e}_0^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{0,\ldots,0,}^{w_0}\ \overbrace{\vec{\eta}_{0,j}}^{z_0})\,\mathbb{B}_0,$$

$s_0 := -a_0(\gamma)$ if $\iota=0,\ s_0 := -b_0(\gamma)$ if $\iota=1,$

$$\boldsymbol{c}_{0,\mu+1}^{(\tau,\kappa,\iota)} := (\overbrace{\delta(s_0+\pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,\ldots,0,}^{u_0}\ \overbrace{0,\ldots0,}^{w_0}\ \overbrace{\vec{\eta}_{0,\mu+1},\ \zeta\chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0,$$

[数183]

$$\text{for } i=1,\ldots,L,$$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i=1,\ldots,L;\ \tau=1,\ldots,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i=1,\ldots,L;\ \iota=0,1),$$

$$s_i := -a_i(\gamma)+\xi_{i,\tau,0} \ \text{ if } \iota=0, \qquad s_i := -b_i(\gamma)+\xi_{i,\tau,1} \ \text{ if } \iota=1,$$

$$\text{if } \rho(i)=(t,\vec{v}_i), \qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q, \quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$$

$$\boldsymbol{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i\vec{e}_1+\theta_i\vec{v}_i),\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{0,\ldots,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})_{\mathbb{B}_t},$$

$$\text{if } \rho(i)=\neg(t,\vec{v}_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{z_t},$$

$$\mathrm{c}_i^{(\tau,\kappa,\iota)} := (\overbrace{\delta s_i\vec{v}_i,\ \vec{e}_i^{(\tau,\kappa,\iota)}}^{n_t},\ \overbrace{0,\ldots,0,}^{u_t}\ \overbrace{0,\ldots,0,}^{w_t}\ \overbrace{\vec{\eta}_i}^{z_t})_{\mathbb{B}_t},$$

$$c_{d+1} := g_T^{\zeta} msg,$$

$$\text{return } \mathrm{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_{0,0}^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{c}_{0,\mu+1}^{(\tau,\kappa,\iota)},$$

$$\mathrm{c}_1^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{c}_L^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1}).$$

[数184]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{ct}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{c}_{0,0}^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{c}_{0,\mu+1}^{(\tau,\kappa,\iota)},\ \boldsymbol{c}_{1}^{(\tau,\kappa,\iota)},\ldots,\boldsymbol{c}_{L}^{(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}, c_{d+1}),\ \mathsf{sk}_{\Gamma} := (\Gamma, \boldsymbol{k}_0^*, \{\boldsymbol{k}_t^*\}_{(t,\vec{x}_t)\in\Gamma})):$$

if $\mathbb{S} := (\mathcal{A}, \mathcal{B}, d(x), \rho)$ accepts $\Gamma := \{(t, \vec{x}_t)\}$,

then compute $I_\delta \subseteq \{1,\ldots,L\}, (\alpha_1,\ldots,\alpha_L), (\beta_1,\ldots,\beta_L)$ and

κ with $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}\, x + \cdots + h_{\tau,\kappa,\iota,\mu}\, x^\mu$

for all $\tau=1,\ldots,m$ and $\iota = 0,1$ such that

$h_{\tau,\kappa,0}(x)\cdot d_\tau(x)^\kappa = a_0(x) + \sum_{i=1}^{L} \alpha_i a_i(x)$, and

$h_{\tau,\kappa,1}(x)\cdot d_\tau(x)^{f_\tau-\kappa} = b_0(x) + \sum_{i=1}^{L} \beta_i b_i(x)$,

$$K_{\tau,0} := e(\boldsymbol{k}_0^*, \sum_{j=0}^{\mu} h_{\tau,\kappa,0,j}\boldsymbol{c}_{0,j}^{(\tau,\kappa,0)})\cdot e(\boldsymbol{k}_0^*, \boldsymbol{c}_{0,\mu+1}^{(\tau,\kappa,0)})\cdot \prod_{i\in I_\delta,+} e(\boldsymbol{k}_t^*, \boldsymbol{c}_i^{(\tau,\kappa,0)})^{\alpha_i}\cdot \prod_{i\in I_\delta,-} e(\boldsymbol{k}_t^*, \boldsymbol{c}_i^{(\tau,\kappa,0)})^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)},$$

$$K_{\tau,1} := e(\boldsymbol{k}_0^*, \sum_{j=0}^{\mu} h_{\tau,\kappa,1,j}\boldsymbol{c}_{0,j}^{(\tau,\kappa,1)})\cdot e(\boldsymbol{k}_0^*, \boldsymbol{c}_{0,\mu+1}^{(\tau,\kappa,1)})\cdot \prod_{i\in I_\delta,+} e(\boldsymbol{k}_t^*, \boldsymbol{c}_i^{(\tau,\kappa,1)})^{\beta_i}\cdot \prod_{i\in I_\delta,-} e(\boldsymbol{k}_t^*, \boldsymbol{c}_i^{(\tau,\kappa,1)})^{\beta_i/(\vec{v}_i\cdot\vec{x}_t)},$$

where $I_{\delta,+} := \{i \in I_\delta \mid \rho(i) = (t, \vec{v}_i)\}$ and $I_{\delta,-} := \{i \in I_\delta \mid \rho(i) = \neg(t, \vec{v}_i)\}$.

return $msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1})$.

[0104] また、関数型暗号方式について説明した。しかし、ＫｅｙＧｅｎアルゴリズム、Ｄｅｃアルゴリズムをそれぞれ数１８５から数１８７に示すようにすることにより、属性ベース暗号方式とすることも可能である。なお、属性ベース暗号方式の場合、Ｓｅｔｕｐアルゴリズムにおいて、n_tは$2mf_{max}k_{max}+2$である。また、Ｓｅｔｕｐアルゴリズムは、数１４９に示すＳｅｔｕｐアルゴリズムと同じであり、Ｅｎｃアルゴリズムは、数１５２に示すＥｎ

cアルゴリズムと同じである。

[数185]

$$\mathsf{KeyGen}\left(\mathsf{pk},\ \mathsf{sk},\ \mathbb{S} := (\mathcal{A},\mathcal{B},d(x)=\prod_{\tau=1}^{m} d_\tau(x)^{f_\tau},\rho)\right):$$

$$\pi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \pi_m := -\sum_{\tau=1}^{m-1}\pi_\tau,$$

$$\pi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \pi_{\tau,\kappa,1} := \pi_\tau - \pi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \kappa=0,...,f_\tau),$$

$$\chi_\tau \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ (\tau=1,...,m-1),\ \ \chi_m := 1-\sum_{\tau=1}^{m-1}\chi_\tau,$$

$$\chi_{\tau,\kappa,0} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \chi_{\tau,\kappa,1} := \chi_\tau - \chi_{\tau,\kappa,0}\ (\tau=1,...,m;\ \kappa=0,...,f_\tau),$$

for $\tau=1,...,m,\ \ \kappa=0,...,f_\tau,\ \ \iota=0,1,$

$$\gamma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \ \vec{\eta}_{0,0},...,\vec{\eta}_{0,\mu+1} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0},$$

for $j=0,...,\mu,$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^\kappa,\ \vec{e}_0^{(\tau,\kappa,0)})}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,...,0}^{z_0})\,\mathbb{B}_0^*,$$

$$\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)} := (\overbrace{\delta(\gamma^j\cdot d_\tau(\gamma)^{f_\tau-\kappa},\ \vec{e}_0^{(\tau,\kappa,1)})}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_{0,j}}^{w_0},\ \overbrace{0,...,0}^{z_0})\,\mathbb{B}_0^*,$$

$s_0 := -a_0(\gamma)$ if $\iota=0$, $s_0 := -b_0(\gamma)$ if $\iota=1$,

$$\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_0+\pi_{\tau,\kappa,\iota},\ \vec{e}_0^{(\tau,\kappa,\iota)})}^{n_0},\ \overbrace{0,...,0}^{u_0},\ \overbrace{\vec{\eta}_{0,\mu+1}}^{w_0},\ \overbrace{0,...0,\ \chi_{\tau,\kappa,\iota}}^{z_0})\,\mathbb{B}_0^*,$$

[数186]

$$\text{for } i=1,\ldots,L,$$

$$\xi_{i,\tau,\iota} \xleftarrow{\cup} \mathbb{F}_q \quad (i=1,\ldots,L;\ \tau=1,\ldots,m-1;\iota=0,1),$$

$$\xi_{i,m,\iota} := -\sum_{\tau=1}^{m-1} \xi_{i,\tau,\iota} \quad (i=1,\ldots,L;\ \iota=0,1),$$

$$s_i := -a_i(\gamma)+\xi_{i,\tau,0} \ \text{ if } \iota=0, \qquad s_i := -b_i(\gamma)+\xi_{i,\tau,1} \ \text{ if } \iota=1,$$

$$\text{if } \rho(i)=(t,v_i), \qquad \theta_i \xleftarrow{\cup} \mathbb{F}_q, \quad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i+\theta_i v_i,\ -\theta_i,\ \vec{e}_i^{(\tau,\kappa,\iota)})}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{if } \rho(i)=\neg(t,v_i), \qquad \vec{\eta}_i \xleftarrow{\cup} \mathbb{F}_q^{w_t},$$

$$\boldsymbol{k}_i^{*(\tau,\kappa,\iota)} := (\overbrace{\delta(s_i v_i,\ s_i,\ \vec{e}_i^{(\tau,\kappa,\iota)})}^{n_t},\ \overbrace{0,\ldots,0}^{u_t},\ \overbrace{\vec{\eta}_i}^{w_t},\ \overbrace{0,\ldots,0}^{z_t})\,\mathbb{B}_t^*,$$

$$\text{return } \mathsf{sk}_{\mathbb{S}} := (\mathbb{S}, \{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},$$

$$\boldsymbol{k}_1^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_L^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}).$$

[数187]

$$\mathsf{Dec}(\mathsf{pk},\ \mathsf{sk}_{\mathbb{S}} := (\mathbb{S},\{\boldsymbol{k}_{0,0}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,\iota)},\ \boldsymbol{k}_{1}^{*(\tau,\kappa,\iota)},\ldots,\boldsymbol{k}_{L}^{*(\tau,\kappa,\iota)}\}_{\tau=1,\ldots,m;\kappa=0,\ldots,f_\tau;\iota=0,1}),$$

$$\mathsf{ct}_{\Gamma} := (\Gamma,\boldsymbol{c}_0,\{\boldsymbol{c}_t\}_{(t,x_t)\in\Gamma},c_{d+1})):$$

if $\mathbb{S} := (\mathcal{A},\mathcal{B},d(x),\ \rho)$ accepts $\Gamma := \{(t,x_t)\}$,

then compute $I_\delta \subseteq \{1,\ldots,L\},(\alpha_1,\ldots,\alpha_L),\ (\beta_1,\ldots,\beta_L)$ and

κ with $h_{\tau,\kappa,\iota}(x) := h_{\tau,\kappa,\iota,0} + h_{\tau,\kappa,\iota,1}\ x + \cdots + h_{\tau,\kappa,\iota,\mu}\ x^{\mu}$

for all $\tau=1,\ldots,m$ and $\iota = 0,1$ such that

$h_{\tau,\kappa,0}(x)\cdot d_\tau(x)^{\kappa} = a_0(x) + \sum_{i=1}^{L}\alpha_i a_i(x)$, and

$h_{\tau,\kappa,1}(x)\cdot d_\tau(x)^{f_\tau-\kappa} = b_0(x) + \sum_{i=1}^{L}\beta_i b_i(x)$,

$$K_{\tau,0} := e(\boldsymbol{c}_0,\sum_{j=0}^{\mu} h_{\tau,\kappa,0,j}\boldsymbol{k}_{0,j}^{*(\tau,\kappa,0)})\cdot e(\boldsymbol{c}_0,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,0)})\cdot \prod_{i\in I_\delta,+} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i}\cdot\prod_{i\in I_\delta,-} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,0)})^{\alpha_i/(v_i-x_t)},$$

$$K_{\tau,1} := e(\boldsymbol{c}_0,\sum_{j=0}^{\mu} h_{\tau,\kappa,1,j}\boldsymbol{k}_{0,j}^{*(\tau,\kappa,1)})\cdot e(\boldsymbol{c}_0,\boldsymbol{k}_{0,\mu+1}^{*(\tau,\kappa,1)})\cdot \prod_{i\in I_\delta,+} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i}\cdot\prod_{i\in I_\delta,-} e(\boldsymbol{c}_t,\boldsymbol{k}_i^{*(\tau,\kappa,1)})^{\beta_i/(v_i-x_t)},$$

where $I_{\delta,+} := \{i\in I_\delta \mid \rho(i) = (t,v_i)\}$ and $I_{\delta,-} := \{i\in I_\delta \mid \rho(i) = \neg(t,v_i)\}$.

return $msg' := c_{d+1} / (\prod_{\tau=1}^{m} K_{\tau,0}K_{\tau,1})$.

同様の変更を行うことにより、数１８１から数１８４に示すＣＰ－ＦＥ方式を属性ベース暗号方式に変更することも可能である。

[0105] また、上記説明では、N_0に$n_0+u_0+w_0+z_0$を設定し、N_tに$n_t+u_t+w_t+z_t$を設定した。ここで、例えば、$u_0=n_0$，$w_0=n_0$，$z_0=2$として、N_0に$n_0+n_0+n_0+2=3n_0+2$とし、$u_t=n_t$，$w_t=n_t$，$z_t=2$として、N_tに$n_t+n_t+n_t+2=3n_t+2$としてもよい。

[0106] また、上記説明では、実施の形態２に係る関数型暗号方式と同様に、復号

鍵や暗号文が長くなる代わりに、基底の数が少ない関数型暗号方式とした。しかし、実施の形態３，４に係る関数型暗号方式に基づき、実施の形態４に係る関数型暗号方式を、実施の形態３に係る関数型暗号方式と同様に、基底の数が多くなる代わりに、各基底の次元数が少ない関数型暗号方式に容易に変形できる。

[0107] また、以上の実施の形態では、ＫＰ－ＦＥ方式とＣＰ－ＦＥ方式とについて説明した。しかし、非特許文献４に記載されたＵｎｉｆｉｅｄ－Ｐｏｌｉｃｙ　ＦＥ（ＵＰ－ＦＥ）方式も、ＫＰ－ＦＥ方式とＣＰ－ＦＥ方式とから容易に構成することができる。

[0108] 実施の形態５．

以上の実施の形態では、双対ベクトル空間において暗号処理を実現する方法について説明した。実施の形態５では、双対加群において暗号処理を実現する方法について説明する。

[0109] つまり、以上の実施の形態では、素数位数ｑの巡回群において暗号プリミティブの処理を実現した。しかし、合成数Ｍを用いて数１８８のように環Ｒを表した場合、環Ｒを係数とする加群においても、上記実施の形態で説明した暗号処理を適用することができる。

[数188]

$$\mathbb{R} := \mathbb{Z}/M\mathbb{Z}$$

ここで、
$\mathbb{Z}$：整数
M：合成数
である。

[0110] 以上の実施の形態で説明したアルゴリズムにおけるF_qをＲに変更すれば、双対加群における暗号プリミティブの処理を実現することができる。

[0111] なお、以上の実施の形態において、安全性の証明の観点から、ｉ＝１，．．．，Ｌの各整数ｉについてのρ（ｉ）は、それぞれ異なる識別情報ｔにつ

いての肯定形の組（ｔ，ｖ→）又は否定形の組￢（ｔ，ｖ→）であると限定してもよい。

言い替えると、ρ（ｉ）＝（ｔ，ｖ→）又はρ（ｉ）＝￢（ｔ，ｖ→）である場合に、関数ρ~を、ρ~（ｉ）＝ｔである｛１，．．．，Ｌ｝→｛１，．．．ｄ｝の写像であるとする。この場合、ρ~が単射であると限定してもよい。なお、ρ（ｉ）は、上述したアクセスストラクチャＳ：＝（Ｍ，ρ（ｉ））のρ（ｉ）である。

[0112] 次に、実施の形態における暗号処理システム１０（鍵生成装置１００、暗号化装置２００、復号装置３００）のハードウェア構成について説明する。

図１３は、鍵生成装置１００、暗号化装置２００、復号装置３００のハードウェア構成の一例を示す図である。

図１３に示すように、鍵生成装置１００、暗号化装置２００、復号装置３００は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、ＬＣＤ９０１（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）、キーボード９０２（Ｋ／Ｂ）、通信ボード９１５、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０（固定ディスク装置）の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。磁気ディスク装置９２０は、所定の固定ディスクインタフェースを介して接続される。

[0113] ＲＯＭ９１３、磁気ディスク装置９２０は、不揮発性メモリの一例である。ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３とＲＡＭ９１４と磁気ディスク装置９２０とは、記憶装置（メモリ）の一例である。また、キーボード９０２、通信ボード９１５は、入力装置の一例である。また、通信ボード９１５は、通信装置の一例である。さらに、ＬＣＤ９０１は、表示装置の一例である。

[0114] 磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

[0115] プログラム群９２３には、上記の説明において「マスター鍵生成部１１０」、「マスター鍵記憶部１２０」、「情報入力部１３０」、「復号鍵生成部１４０」、「鍵配布部１５０」、「公開パラメータ取得部２１０」、「情報入力部２２０」、「暗号化データ生成部２３０」、「データ送信部２４０」、「情報取得部３１０」、「スパンプログラム計算部３２０」、「補完係数計算部３３０」、「復号部３４０」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、上記の説明において「公開パラメータｐｋ」、「マスター秘密鍵ｓｋ」、「復号鍵sk_S，sk_Γ」、「暗号文ct_Γ，ct_S」、「アクセスストラクチャＳ」、「属性情報」、「メッセージｍｓｇ」等の情報やデータや信号値や変数値やパラメータが、「ファイル」や「データベース」の各項目として記憶される。「ファイル」や「データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１の動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

[0116] また、上記の説明におけるフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、その他

光ディスク等の記録媒体やＩＣチップに記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体や電波によりオンライン伝送される。

また、上記の説明において「～部」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。また、「～装置」として説明するものは、「～回路」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。さらに、「～処理」として説明するものは「～ステップ」であっても構わない。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、ＲＯＭ９１３等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、上記で述べた「～部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた「～部」の手順や方法をコンピュータ等に実行させるものである。

符号の説明

[0117] １００　鍵生成装置、１１０　マスター鍵生成部、１２０　マスター鍵記憶部、１３０　情報入力部、１４０　復号鍵生成部、１４１　秘密情報生成部、１４２　鍵要素生成部、１５０　鍵配布部、２００　暗号化装置、２１０　公開パラメータ取得部、２２０　情報入力部、２３０　暗号化データ生成部、２４０　データ送信部、３００　復号装置、３１１　復号鍵取得部、３１２　暗号文取得部、３２０　スパンプログラム計算部、３３０　補完係数計算部、３３１　多項式選択部、３３２　係数計算部、３４０　復号部、３４１　ペアリング演算部、３４２　メッセージ計算部。

請求の範囲

[請求項1] ２次スパンプログラムを含む第１情報と、属性情報を含む第２情報とのうちの一方を暗号文として生成する暗号化装置と、

前記第１情報と前記第２情報とのうちの他方を復号鍵とし、前記２次スパンプログラムが前記属性情報を受理する場合に前記２次スパンプログラムと前記属性情報とから得られる情報に基づき、前記暗号文を復号する復号装置と

を備えることを特徴とする暗号システム。

[請求項2] 前記第１情報は、前記２次スパンプログラムとして、多項式ｄ（ｘ）と複数の多項式D_i（ｘ）と述語情報とを含み、

前記復号装置は、

前記第１情報に含まれる述語情報と、前記第２情報に含まれる属性情報とに基づき、前記複数の多項式D_i（ｘ）から少なくとも一部の多項式D_i（ｘ）を選択する多項式選択部と、

前記多項式選択部が選択した多項式D_i（ｘ）に係数Δ_iを掛けた多項式$\Delta_i D_i$（ｘ）に基づき構成される多項式を、前記多項式ｄ（ｘ）で割り切れるようにする係数Δ_iを計算する係数計算部と、

前記係数計算部が計算した係数Δ_iに基づき、前記暗号文を復号する復号部と

を備えることを特徴とする請求項１に記載の暗号システム。

[請求項3] 前記複数の多項式D_i（ｘ）は、ｉ＝０，．．．，Ｌ（Ｌは１以上の整数）の各整数ｉについての多項式a_i（ｘ）及び多項式b_i（ｘ）であり、

前記多項式選択部は、前記属性情報と前記述語情報とに基づき、ｉ＝１，．．．，Ｌのうち一部の整数ｉの集合Ｉを選択することにより、多項式a_0（ｘ）及び多項式b_0（ｘ）と、前記集合Ｉに含まれる整数ｉについての多項式a_i（ｘ）及び多項式b_i（ｘ）とを選択し、

前記係数計算部は、（$a_0(x)+\Sigma_{i\in I}\alpha_i a_i(x)$）・（$b_0(x)+\Sigma_{i\in I}\beta_i b_i(x)$）を前記多項式ｄ（ｘ）で割り切れるようにする係数$\alpha_i$及び係数$\beta_i$を前記係数$\Delta_i$として計算する

ことを特徴とする請求項２に記載の暗号システム。

［請求項4］ 前記多項式ｄ（ｘ）は、$\tau=1,\ldots,m$（ｍは１以上の整数）の多項式$d_\tau(x)^{f_\tau}$に因数分解され、

前記係数計算部は、$\Pi_{\tau=1}^{m} d_\tau(x)^{\kappa_\tau}$が（$a_0(x)+\Sigma_{i\in I}\alpha_i a_i(x)$）を割り切るようにするとともに、$\Pi_{\tau=1}^{m} d_\tau(x)^{f_\tau-\kappa_\tau}$が（$b_0(x)+\Sigma_{i\in I}\beta_i b_i(x)$）を割り切るようにする係数$\alpha_i$及び係数$\beta_i$と、次数$\kappa_\tau$とを計算し、

前記復号部は、前記係数α_i及び前記係数β_iと、前記次数κ_τとに基づき、前記暗号文を復号する

ことを特徴とする請求項３に記載の暗号システム。

［請求項5］ 前記属性情報は、ｔ＝１，．．．，ｄ（ｄは１以上の整数）の少なくとも一部の整数ｔについての属性ベクトル$\vec{x}_t$を含み、

前記述語情報は、ｉ＝１，．．．，Ｌの各整数ｉについての識別子ｔと述語ベクトル$\vec{v}_i$との組（ｔ，$\vec{v}_i$）を含み、

前記多項式選択部は、ｉ＝１，．．．，Ｌの各整数ｉについての前記組（ｔ，$\vec{v}_i$）について、その組の述語ベクトル$\vec{v}_i$とその組の識別情報ｔについての属性ベクトル$\vec{x}_t$との内積が０となるか否かにより、整数ｉを前記集合Ｉに含めるか否かを判定する

ことを特徴とする請求項３又は４に記載の暗号システム。

［請求項6］ 前記組（ｔ，$\vec{v}_i$）は、肯定形と否定形とのいずれかに対応付けられており、

前記多項式選択部は、前記組（ｔ，$\vec{v}_i$）が肯定形に対応付けられている場合、前記内積が０となるなら、整数ｉを前記集合Ｉに含め、前記組（ｔ，$\vec{v}_i$）が否定形に対応付けられている場合、前記内積が０とならないなら、整数ｉを前記集合Ｉに含める

ことを特徴とする請求項５に記載の暗号システム。

[請求項7] 前記多項式ｄ（ｘ）は、τ＝１，．．．，ｍ（ｍは１以上の整数）の多項式$d_{\tau}(x)^{f_{\tau}}$に因数分解され、

前記第１情報は、多項式$d_{\tau}(x)^{f_{\tau}}$毎に、その多項式$d_{\tau}(x)^{f_{\tau}}$によって得られる情報が設定された要素を含み、

前記復号部は、前記係数Δ_iと前記要素とに基づき、前記暗号文を復号する

ことを特徴とする請求項２から６までのいずれかに記載の暗号システム。

[請求項8] 前記第１情報は、多項式$d_{\tau}(x)^{f_{\tau}}$毎に、κ＝０，．．．，f_{τ}の各整数κと、ｉ＝０，．．．，Ｌの各整数ｉとについて、多項式$d_{\tau}(x)^{\kappa}$で多項式$a_i(x)$を割った余りを設定した要素と、多項式$d_{\tau}(x)^{f_{\tau}-\kappa}$で多項式$b_i(x)$を割った余りを設定した要素とを含む

ことを特徴とする請求項７に記載の暗号システム。

[請求項9] 前記第１情報は、多項式$d_{\tau}(x)^{f_{\tau}}$毎に、所定の値γを代入した値を設定した要素を含む

ことを特徴とする請求項７に記載の暗号システム。

[請求項10] 前記復号部は、前記係数Δ_iに基づき、前記要素について所定の演算を行うことにより、前記多項式$d_{\tau}(x)^{f_{\tau}}$によって得られる情報を０にして、前記暗号文を復号する

ことを特徴とする請求項７から９までのいずれかに記載の暗号システム。

[請求項11] 暗号化装置が、２次スパンプログラムを含む第１情報と、属性情報を含む第２情報とのうちの一方を暗号文として生成する暗号化工程と、

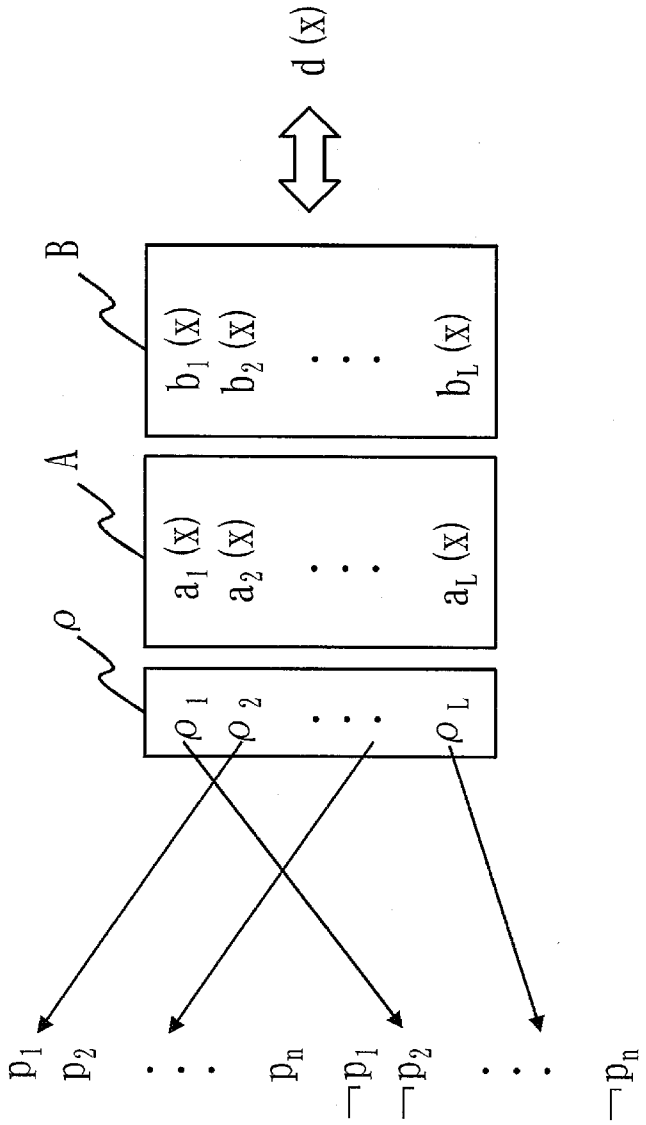
復号装置が、前記第１情報と前記第２情報とのうちの他方を復号鍵とし、前記２次スパンプログラムが前記属性情報を受理する場合に前

記２次スパンプログラムと前記属性情報とから得られる情報に基づき、前記暗号文を復号する復号工程と
を備えることを特徴とする暗号方法。

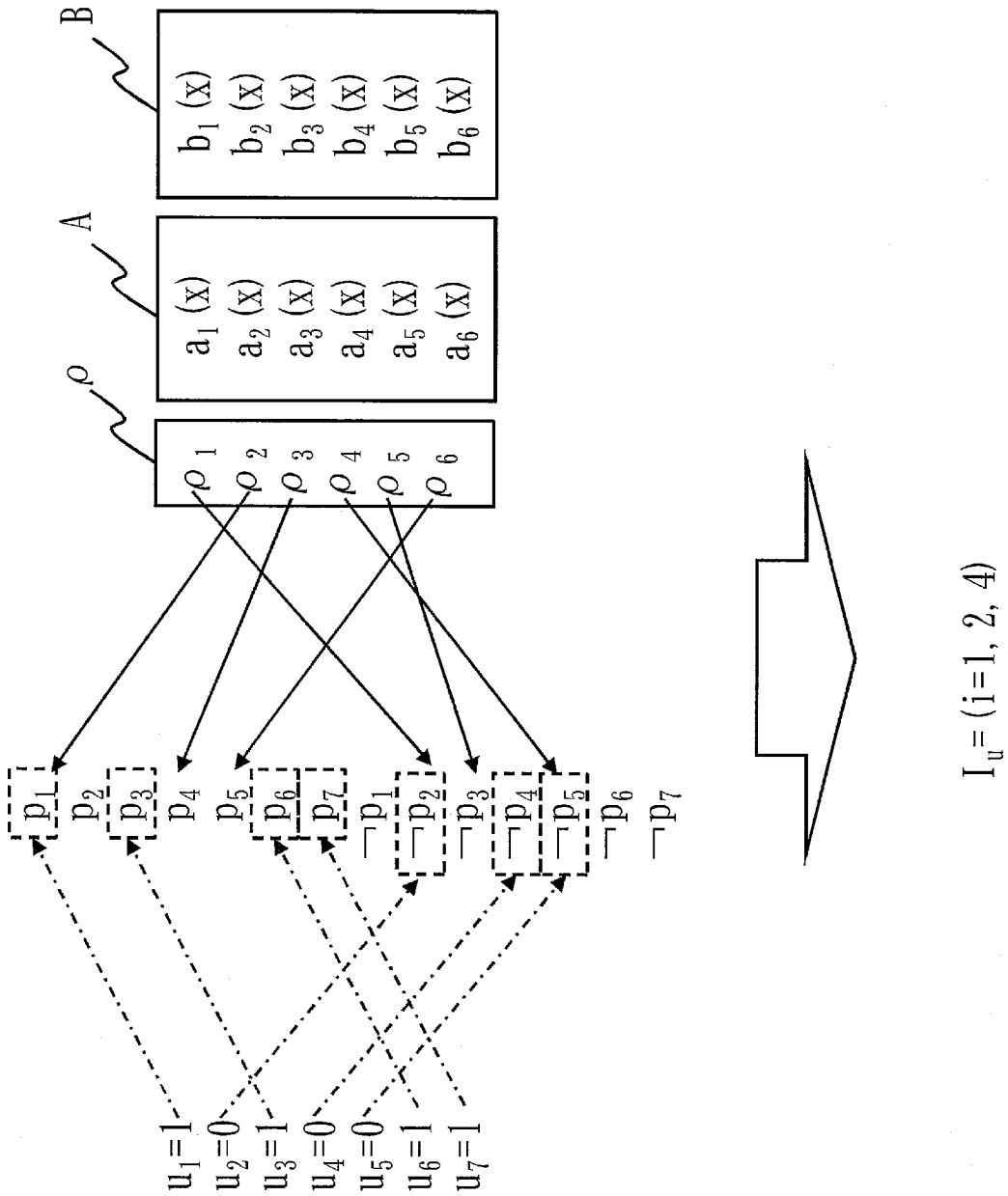
［請求項12］ ２次スパンプログラムを含む第１情報と、属性情報を含む第２情報とのうちの一方を暗号文として生成する暗号化処理と、
前記第１情報と前記第２情報とのうちの他方を復号鍵とし、前記２次スパンプログラムが前記属性情報を受理する場合に前記２次スパンプログラムと前記属性情報とから得られる情報に基づき、前記暗号文を復号する復号処理と
をコンピュータに実行させることを特徴とする暗号プログラム。

［請求項13］ ２次スパンプログラムを含む第１情報と、属性情報を含む第２情報とのうちの一方を暗号文とし、他方を復号鍵として取得する情報取得部と、
前記情報取得部が取得した第１情報に含まれる２次スパンプログラムが第２情報に含まれる属性情報を受理する場合に前記２次スパンプログラムと前記属性情報とから得られる情報に基づき、前記暗号文を復号する復号部と
を備えることを特徴とする復号装置。

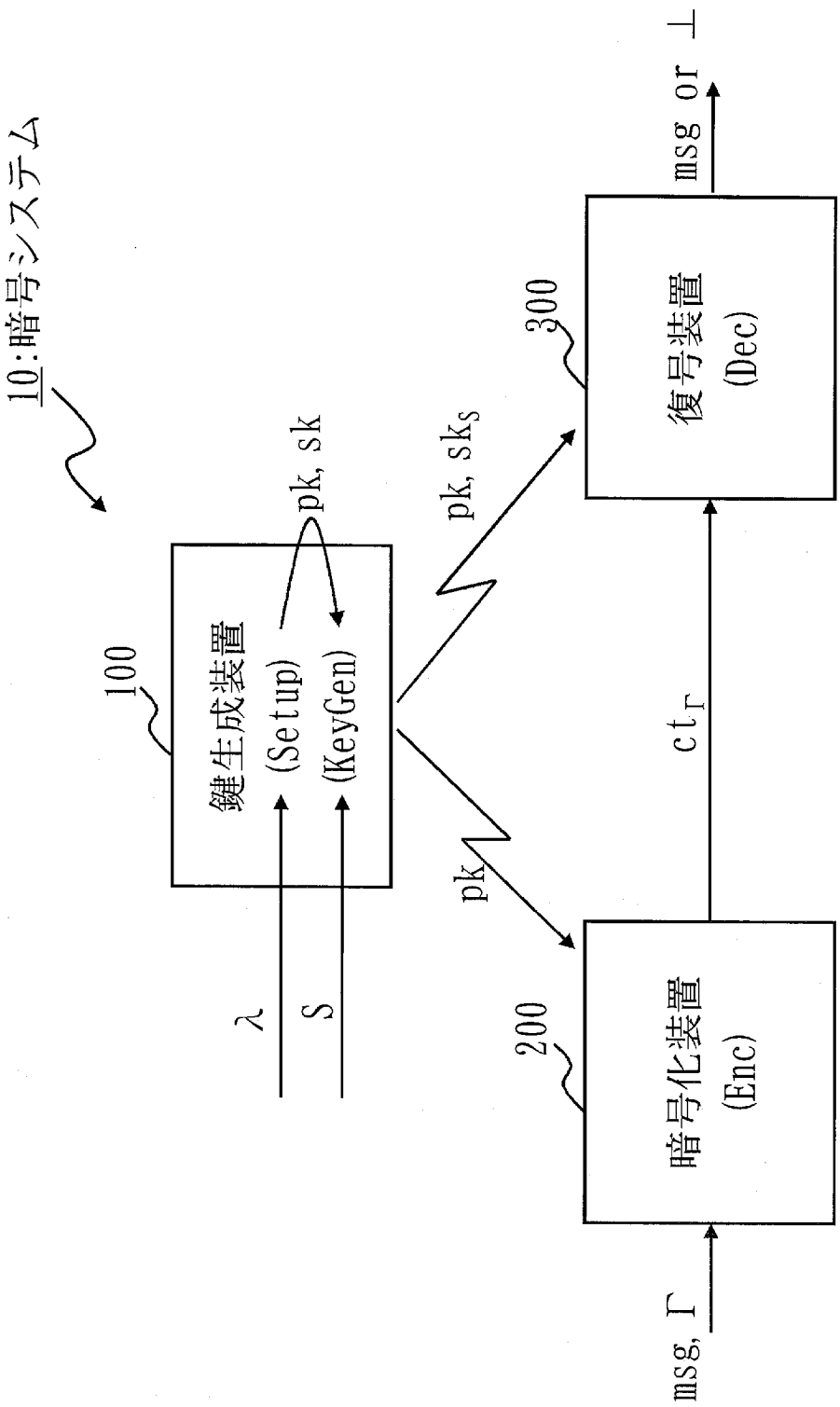
[図1]



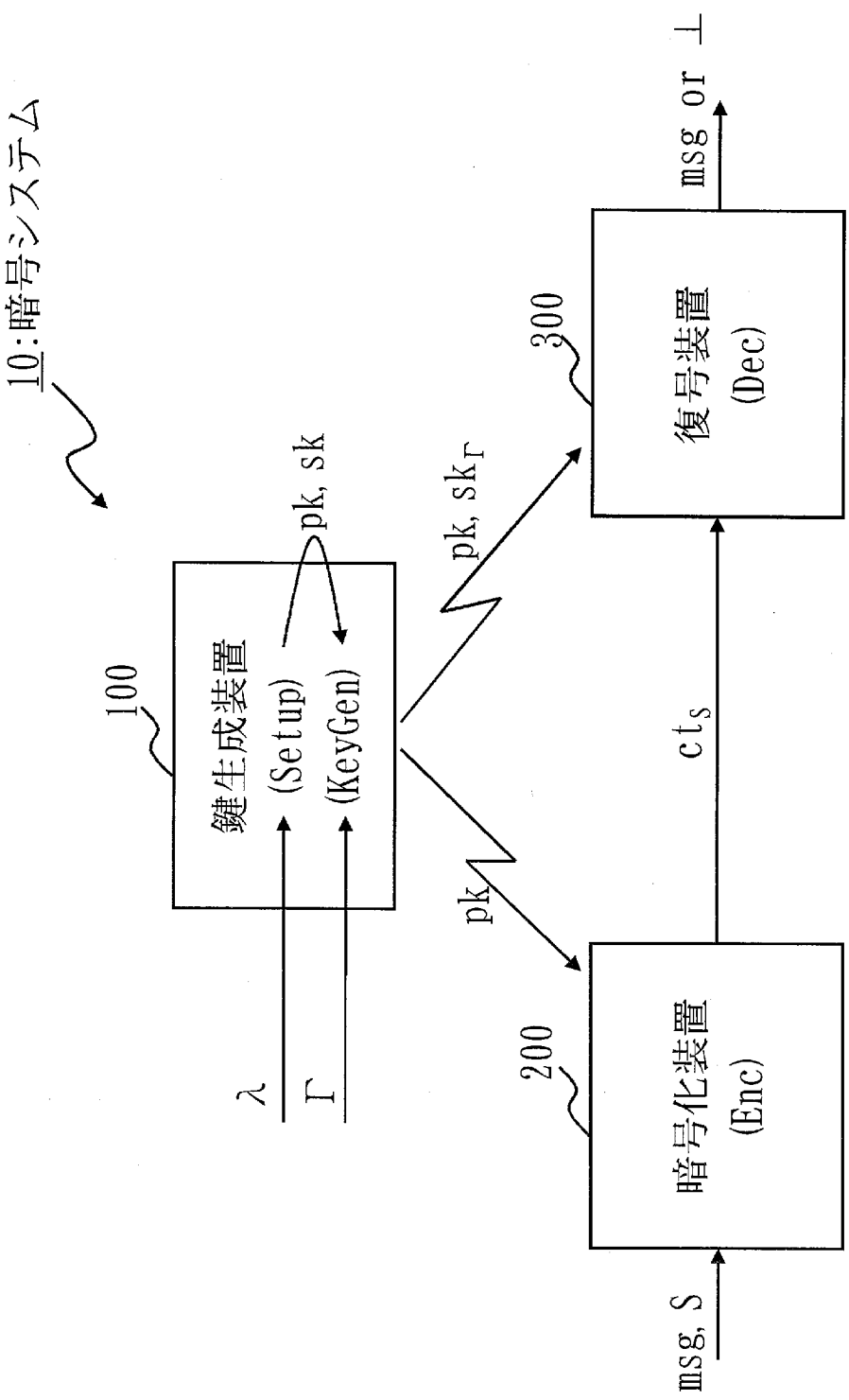
[図2]


B
$b_1(x)$ $b_2(x)$ $b_3(x)$ $b_4(x)$ $b_5(x)$ $b_6(x)$
A
$a_1(x)$ $a_2(x)$ $a_3(x)$ $a_4(x)$ $a_5(x)$ $a_6(x)$
ρ
ρ_1 ρ_2 ρ_3 ρ_4 ρ_5 ρ_6
p_1 p_2 p_3 p_4 p_5 p_6 p_7 $\neg p_1$ $\neg p_2$ $\neg p_3$ $\neg p_4$ $\neg p_5$ $\neg p_6$ $\neg p_7$
$u_1=1$ $u_2=0$ $u_3=1$ $u_4=0$ $u_5=0$ $u_6=1$ $u_7=1$
$I_u = (i=1, 2, 4)$

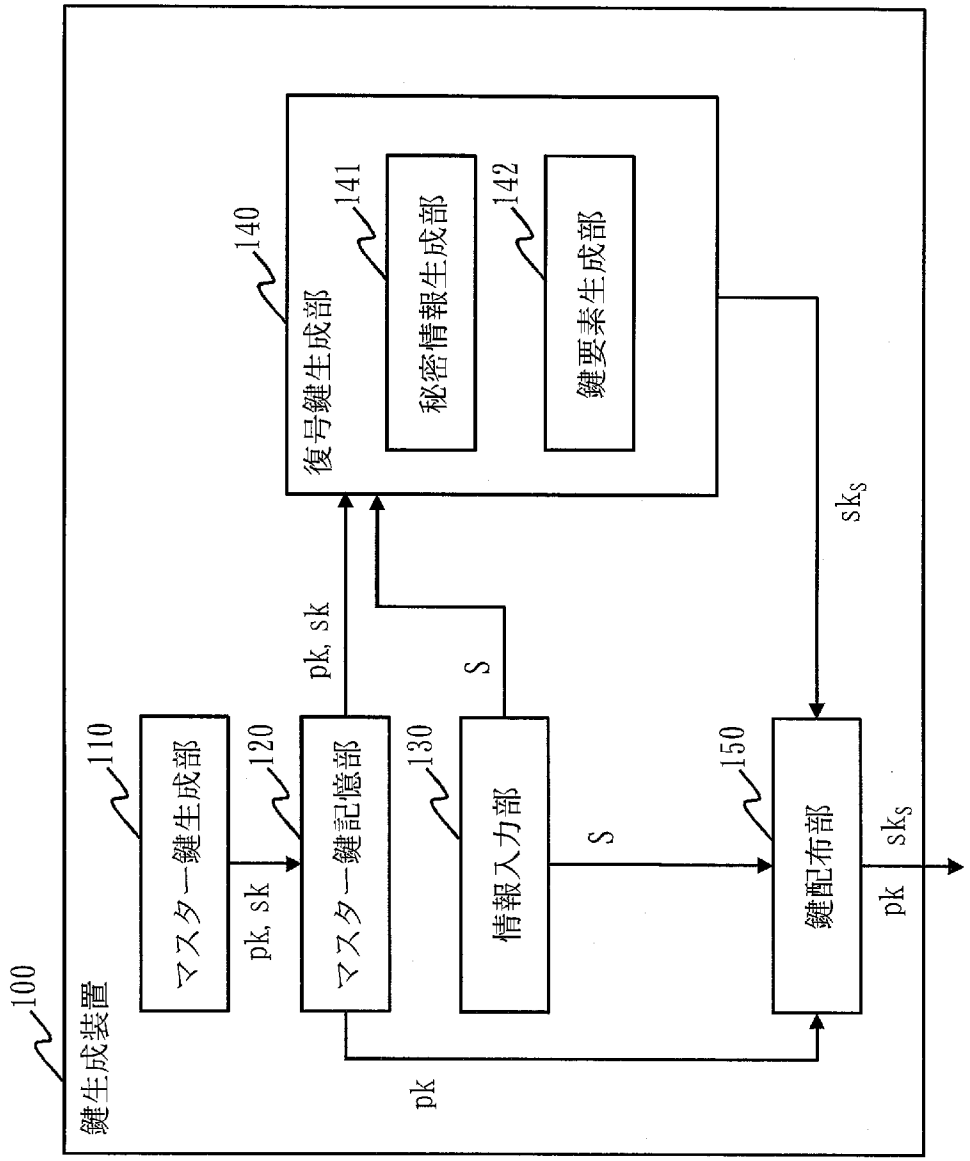
[図3]


10:暗号システム
100
鍵生成装置
(Setup)
(KeyGen)
λ
S
pk, sk
pk, sk_S
pk
200
暗号化装置
(Enc)
msg, Γ
ct_Γ
300
復号装置
(Dec)
msg or ⊥

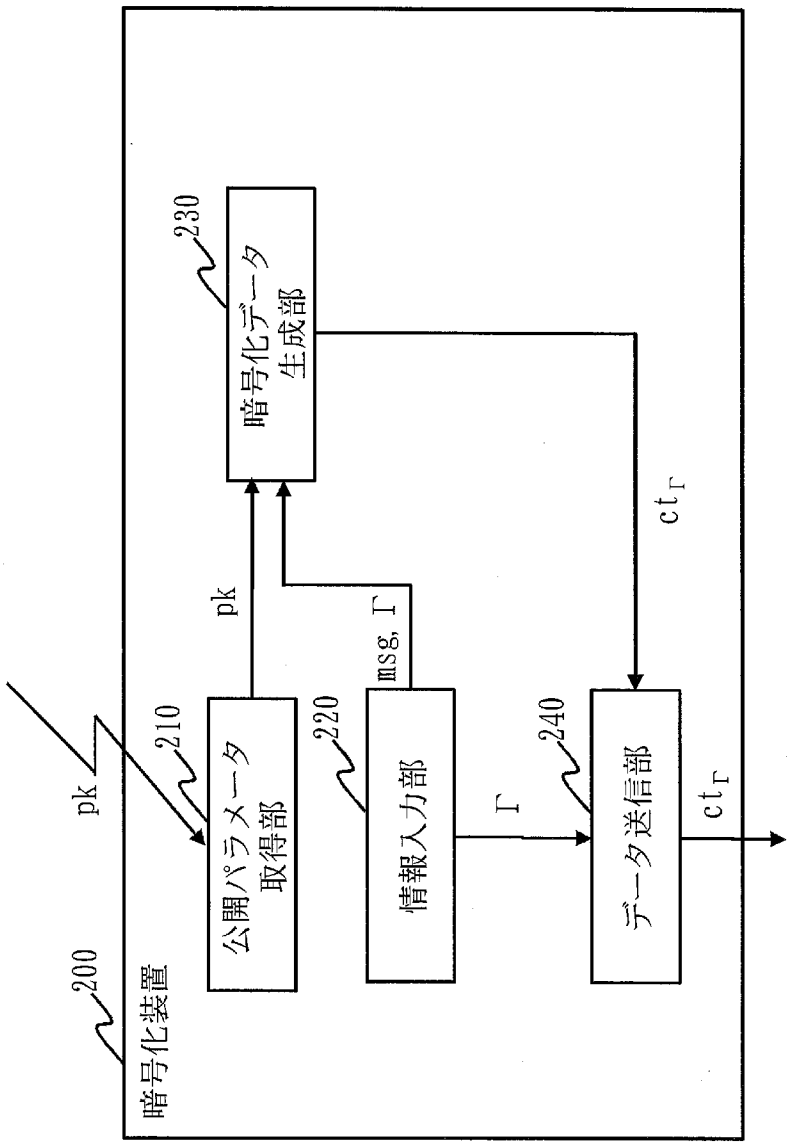
[図4]


10:暗号システム
100
鍵生成装置
(Setup)
(KeyGen)
pk, sk
λ
Γ
pk, skΓ
pk
300
復号装置
(Dec)
msg or ⊥
ct_S
200
暗号化装置
(Enc)
msg, S

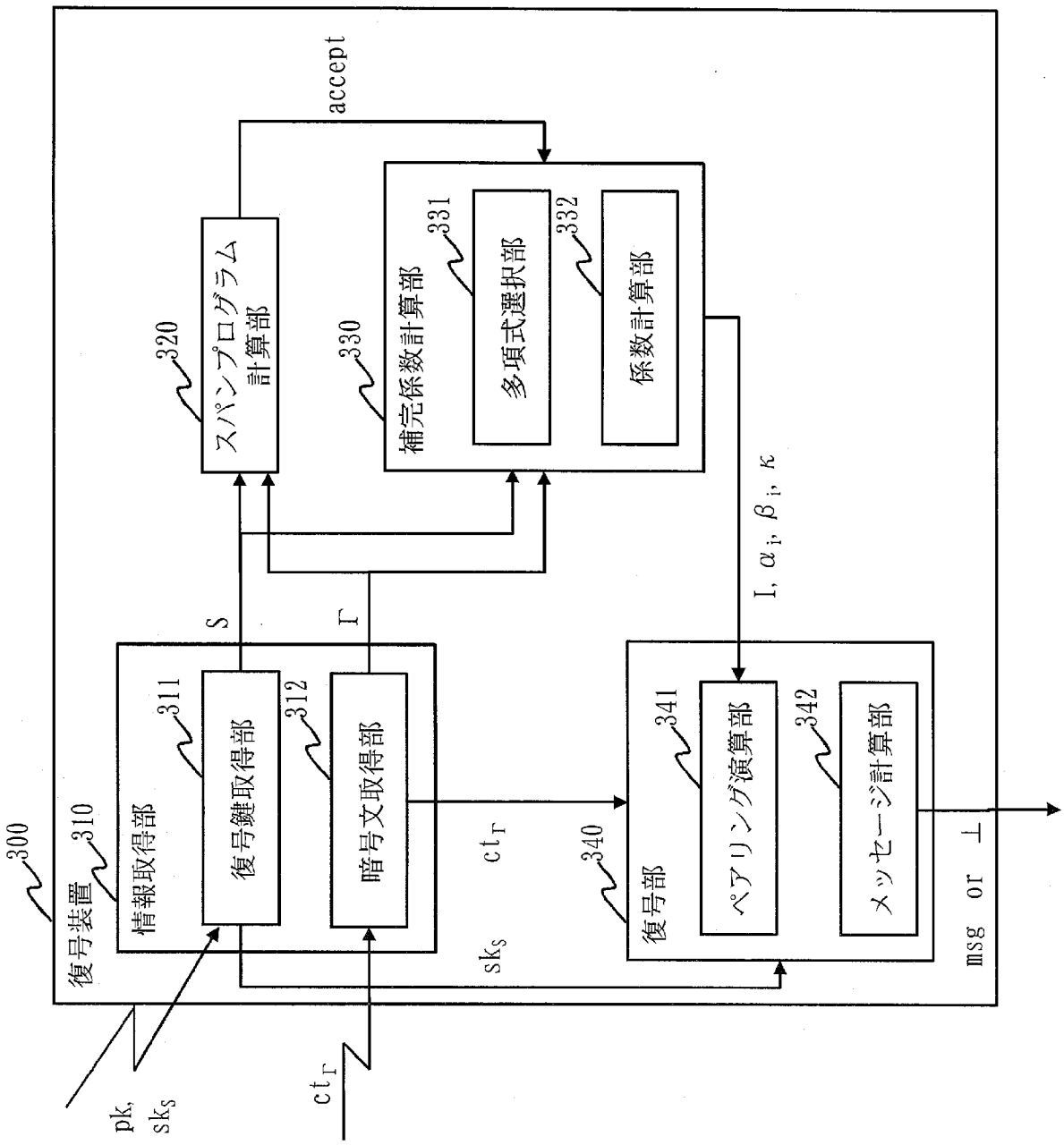
[図5]


100
鍵生成装置
110
マスター鍵生成部
120
マスター鍵記憶部
130
情報入力部
140
復号鍵生成部
141
秘密情報生成部
142
鍵要素生成部
150
鍵配布部
pk, sk
pk, sk
S
S
pk
pk
sk_S
sk_S

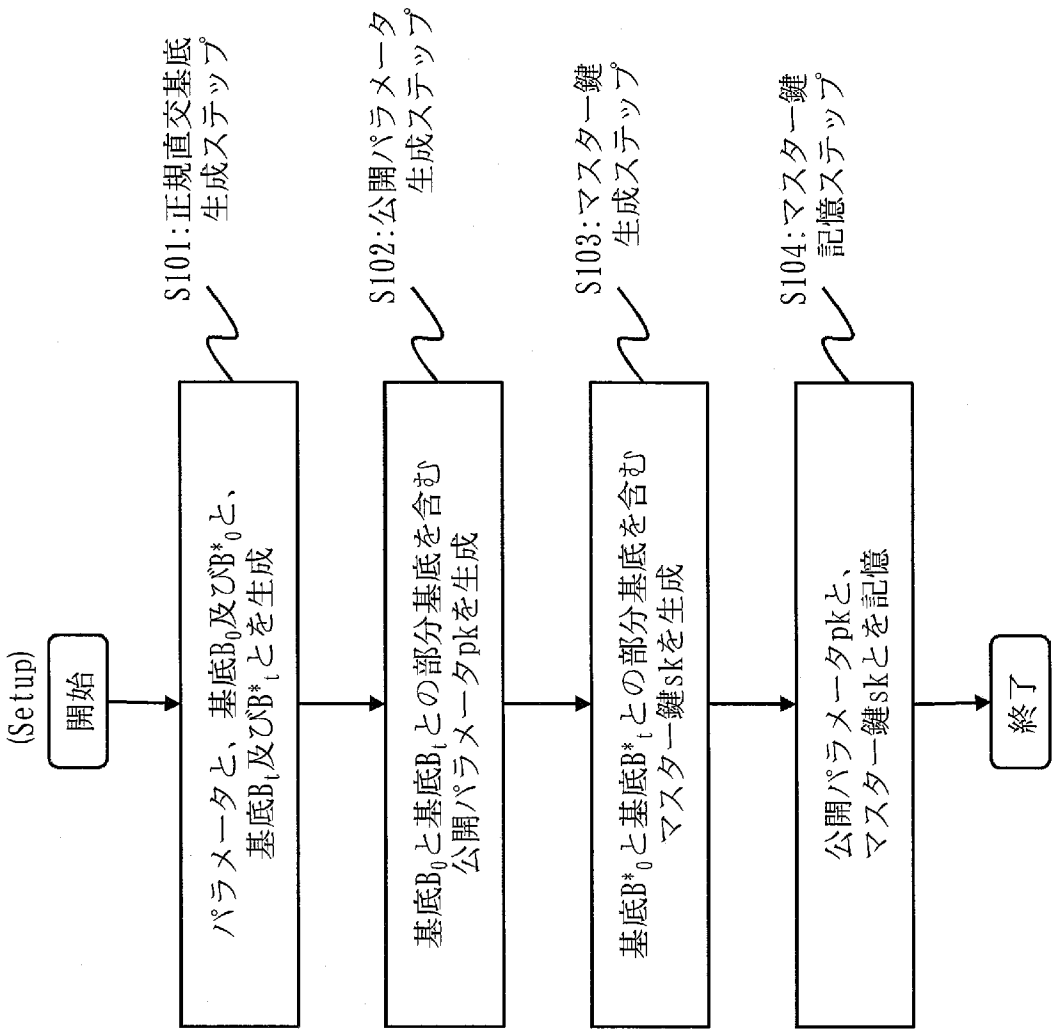
[図6]


暗号化装置
200
公開パラメータ取得部
210
情報入力部
220
データ送信部
240
暗号化データ生成部
230
pk
pk
msg, Γ
Γ
ct_Γ
ct_Γ

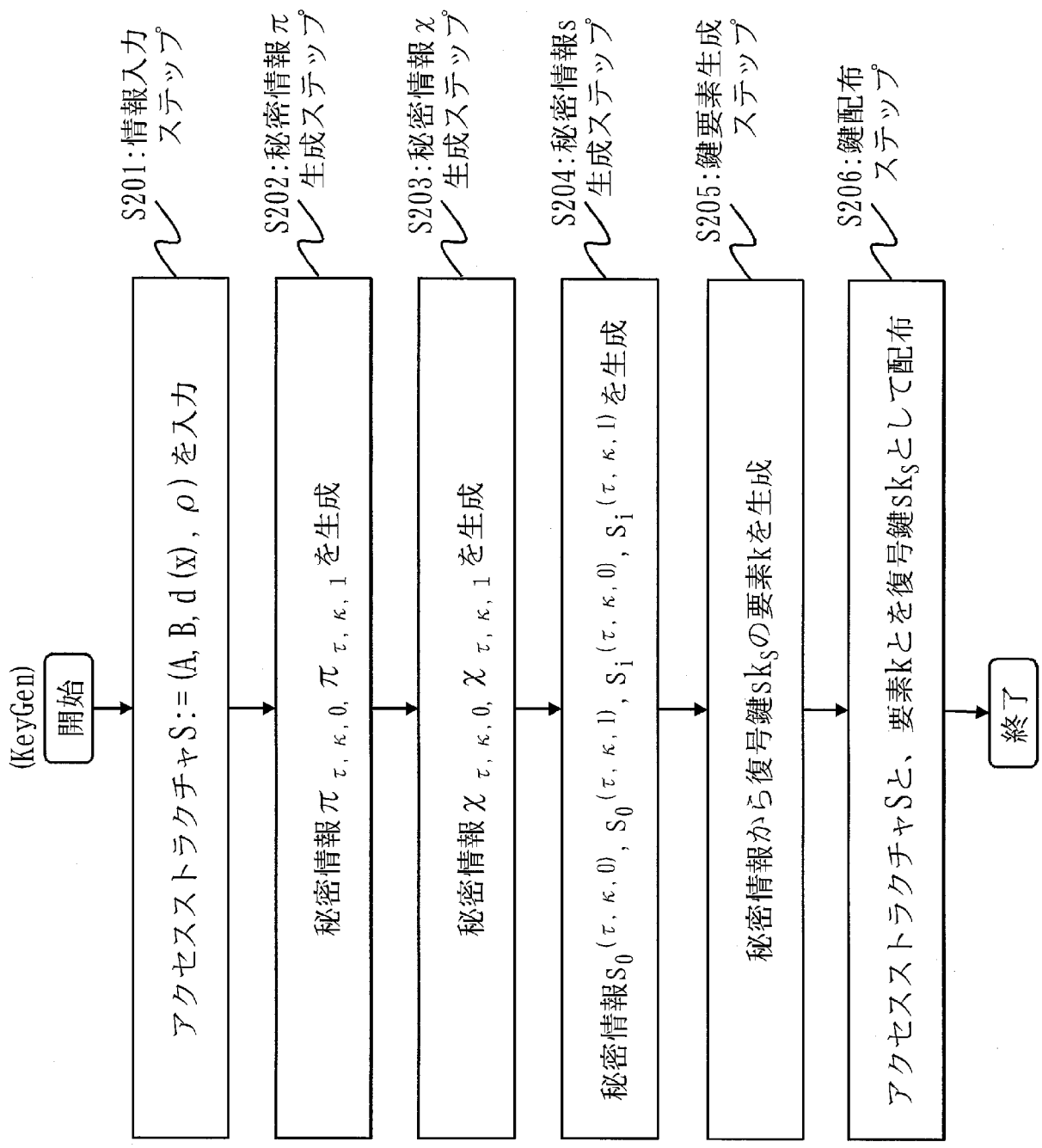
[図7]


300
復号装置
310
情報取得部
311
復号鍵取得部
312
暗号文取得部
320
スパンプログラム計算部
330
補完係数計算部
331
多項式選択部
332
係数計算部
340
復号部
341
ペアリング演算部
342
メッセージ計算部
accept
S
Γ
I, α_i, β_i, κ
sk_S
ct_Γ
pk,
sk_S
ct_Γ
msg or ⊥

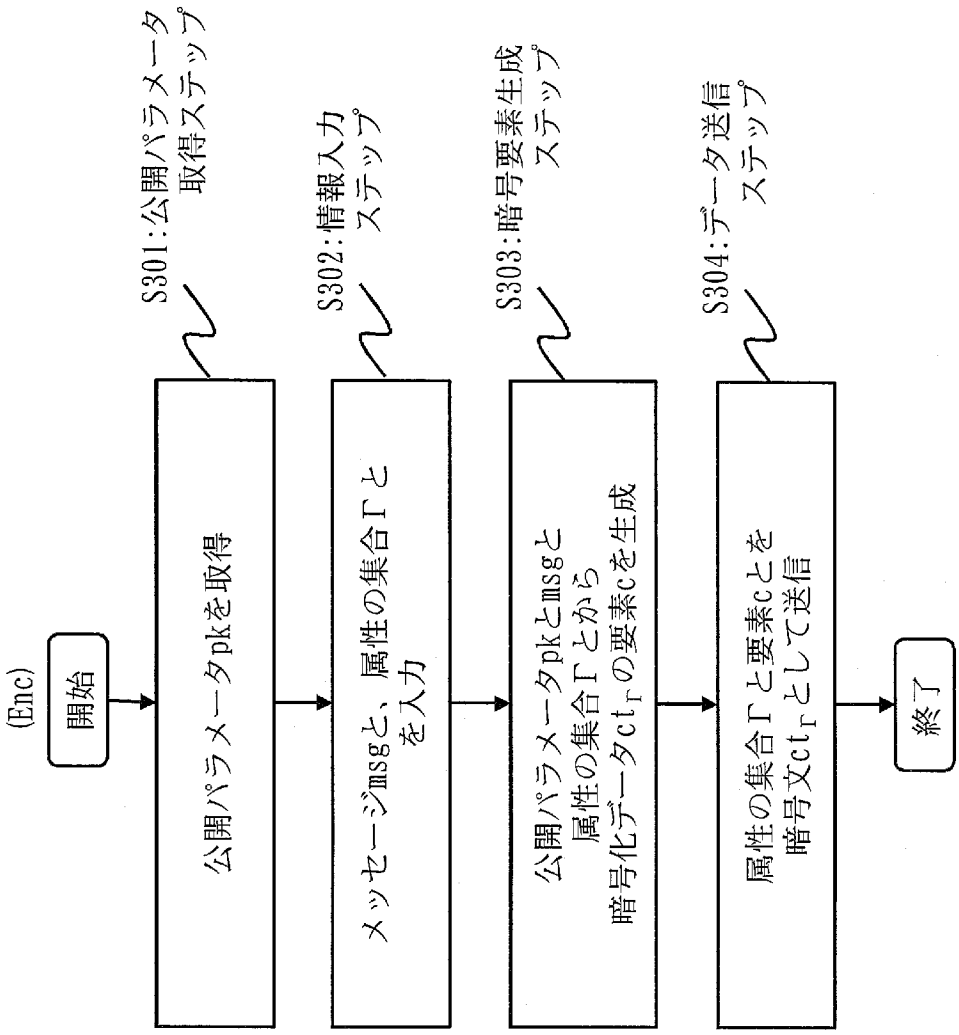
[図8]


(Setup)
開始
S101:正規直交基底
生成ステップ
パラメータと、基底B_0及びB^*_0と、
基底B_t及びB^*_tとを生成
S102:公開パラメータ
生成ステップ
基底B_0と基底B_tとの部分基底を含む
公開パラメータpkを生成
S103:マスター鍵
生成ステップ
基底B^*_0と基底B^*_tとの部分基底を含む
マスター鍵skを生成
S104:マスター鍵
記憶ステップ
公開パラメータpkと、
マスター鍵skとを記憶
終了

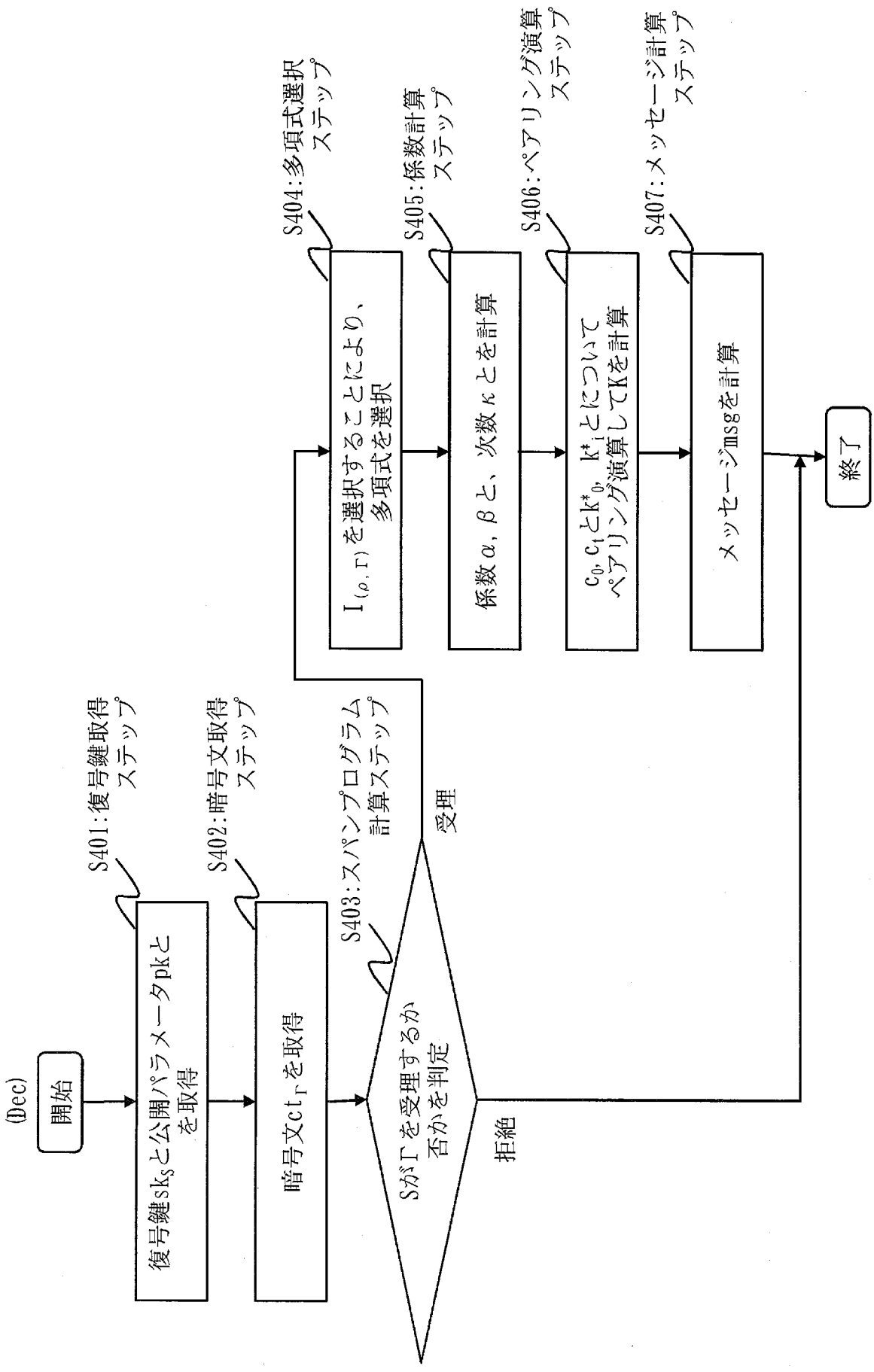
[図9]


(KeyGen)
開始
S201:情報入力ステップ
アクセスストラクチャS:=(A, B, d(x), ρ)を入力
S202:秘密情報π生成ステップ
秘密情報$\pi_{\tau,\kappa,0}$, $\pi_{\tau,\kappa,1}$を生成
S203:秘密情報χ生成ステップ
秘密情報$\chi_{\tau,\kappa,0}$, $\chi_{\tau,\kappa,1}$を生成
S204:秘密情報s生成ステップ
秘密情報$S_0^{(\tau,\kappa,0)}$, $S_0^{(\tau,\kappa,1)}$, $S_i^{(\tau,\kappa,0)}$, $S_i^{(\tau,\kappa,1)}$を生成
S205:鍵要素生成ステップ
秘密情報から復号鍵sk_Sの要素kを生成
S206:鍵配布ステップ
アクセスストラクチャSと、要素kとを復号鍵sk_Sとして配布
終了

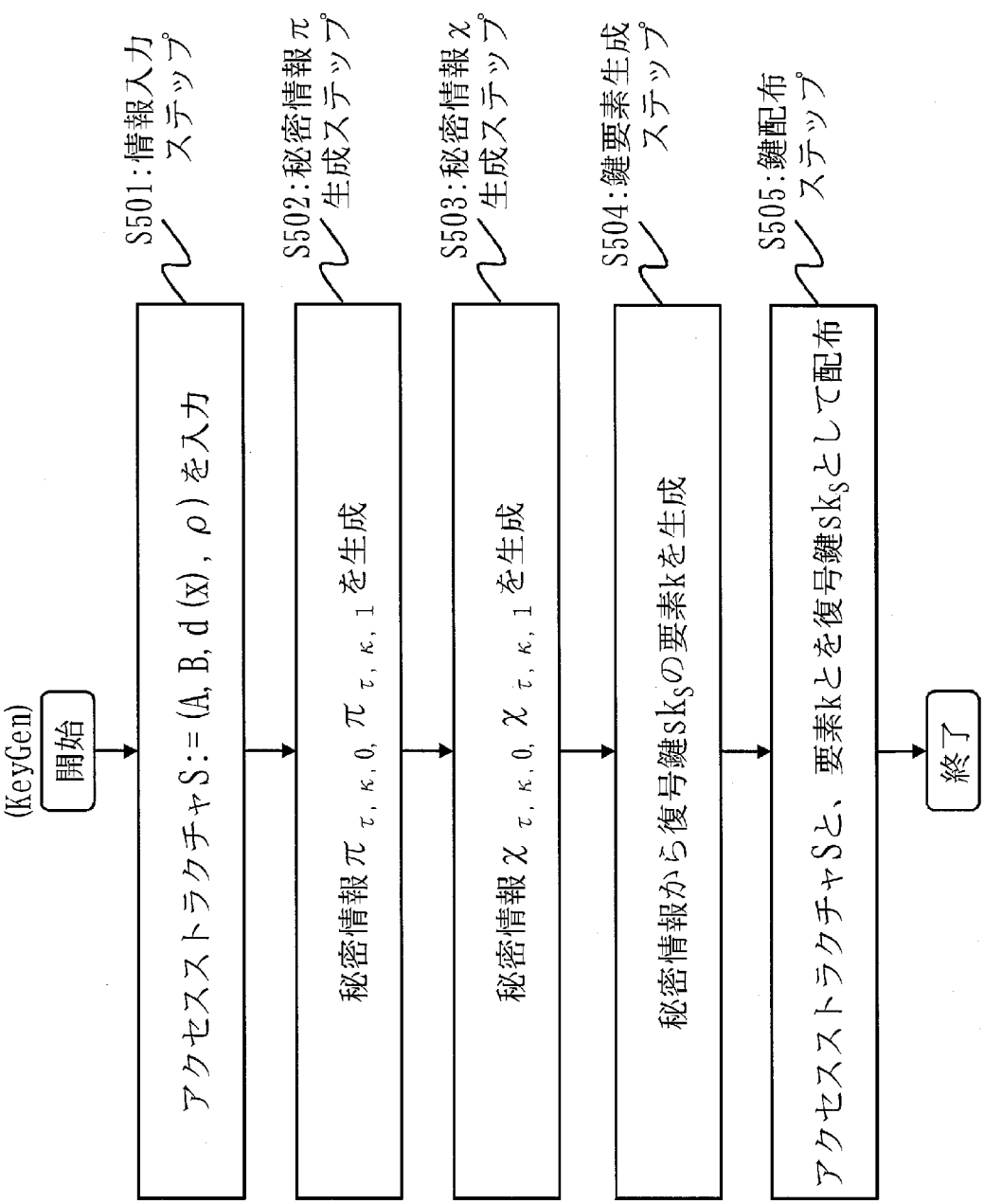
[図10]


(Enc)
開始
公開パラメータpkを取得
S301:公開パラメータ取得ステップ
メッセージmsgと、属性の集合Γとを入力
S302:情報入力ステップ
公開パラメータpkとmsgと属性の集合Γとから暗号化データct_Γの要素cを生成
S303:暗号要素生成ステップ
属性の集合Γと要素cとを暗号文ct_Γとして送信
S304:データ送信ステップ
終了

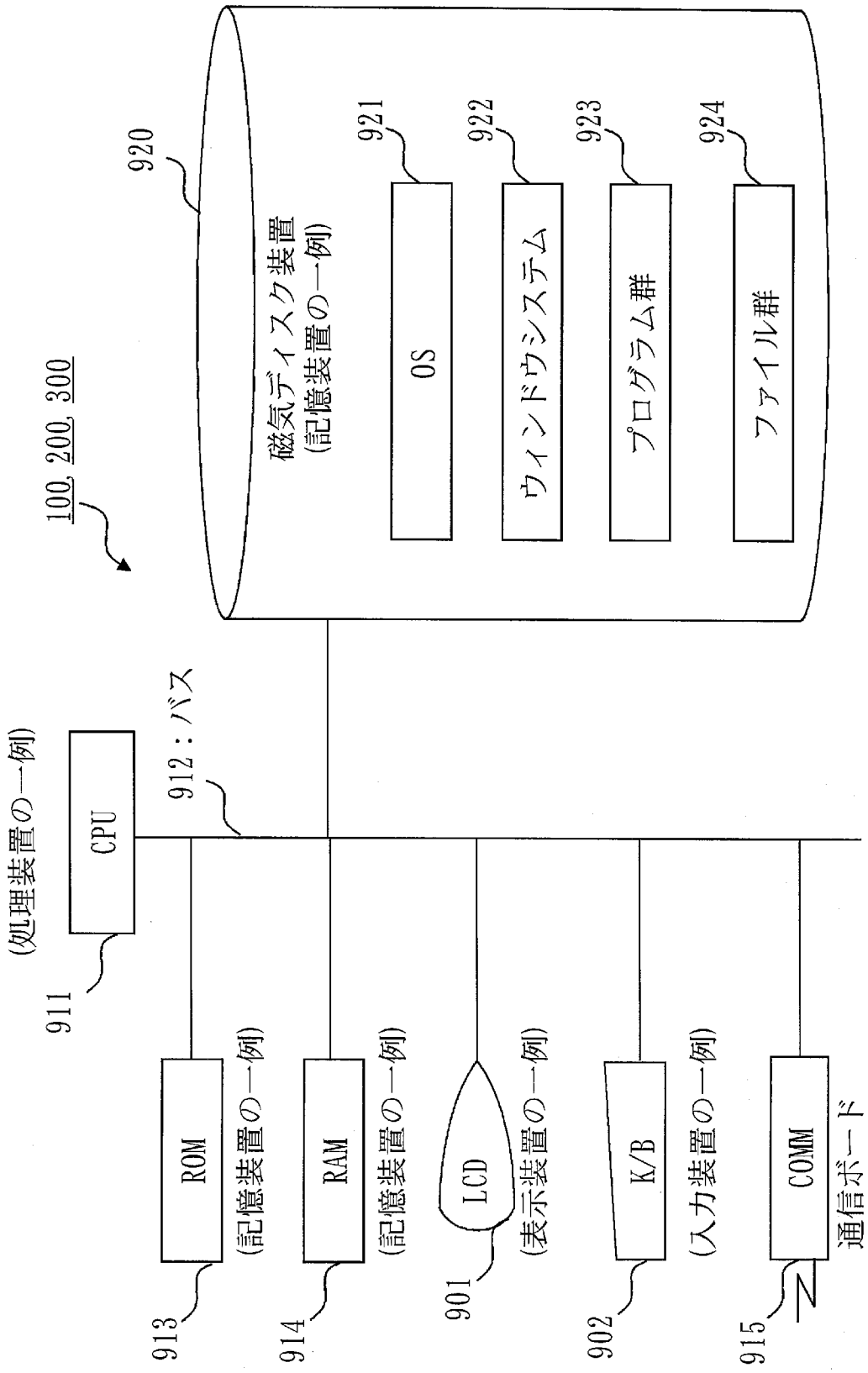
[図11]


(Dec)
開始
復号鍵sk_Sと公開パラメータpkと
を取得
S401:復号鍵取得
ステップ
暗号文ct_Γを取得
S402:暗号文取得
ステップ
SがΓを受理するか
否かを判定
S403:スパンプログラム
計算ステップ
受理
拒絶
$I_{(\rho,\Gamma)}$を選択することにより、
多項式を選択
S404:多項式選択
ステップ
係数α, βと、次数κとを計算
S405:係数計算
ステップ
c_0, c_tとk^*_0, k^*_iとについて
ペアリング演算してKを計算
S406:ペアリング演算
ステップ
メッセージmsgを計算
S407:メッセージ計算
ステップ
終了

[図12]


(KeyGen)
開始
S501:情報入力ステップ
アクセスストラクチャS:=(A, B, d(x), ρ)を入力
S502:秘密情報πの生成ステップ
秘密情報 $\pi_{\tau,\kappa,0}$, $\pi_{\tau,\kappa,1}$ を生成
S503:秘密情報χの生成ステップ
秘密情報 $\chi_{\tau,\kappa,0}$, $\chi_{\tau,\kappa,1}$ を生成
S504:鍵要素生成ステップ
秘密情報から復号鍵sk_Sの要素kを生成
S505:鍵配布ステップ
アクセスストラクチャSと、要素kとを復号鍵sk_Sとして配布
終了

[図13]


100, 200, 300
920
磁気ディスク装置
(記憶装置の一例)
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
912：バス
(処理装置の一例)
CPU
911
ROM
(記憶装置の一例)
913
RAM
(記憶装置の一例)
914
LCD
(表示装置の一例)
901
K/B
(入力装置の一例)
902
COMM
通信ボード
915

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/069368

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i

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

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IEEE Xplore, THE ACM DIGITAL LIBRARY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2011-232475 A (Mitsubishi Electric Corp.), 17 November 2011 (17.11.2011), paragraphs [0023] to [0027], [0039] to [0040], [0050] to [0073], [0081] to [0106], [0155] to [0164]; fig. 1 to 2, 5 to 15 & US 2013/0028415 A1 & EP 2565862 A1 & WO 2011/135895 A1 & CN 102859571 A & KR 10-2012-0139753 A	1,11-13 2-10
Y A	Tatsuaki Okamoto et al, Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, [online], 2011.12.22, [Retrieval date 02 August 2013 (02.08.2013)], Internet <URL:https://eprint.iacr.org/2010/563>	1,11-13 2-10

☒ 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
"T" 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	Date of mailing of the international search report
02 August, 2013 (02.08.13)	13 August, 2013 (13.08.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/069368

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	Rosario Gennaro et al, Quadratic Span Programs and Succinct NIZKs without PCPs, [online], 2012. 06.18, [Retrieval date 02 August 2013 (02.08. 2013)], Internet <URL:https://eprint.iacr.org/ 2012/215>	1,11-13 2-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０６９３６８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i

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））

Int.Cl.　G09C1/00

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

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

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）

IEEE Xplore, THE ACM DIGITAL LIBRARY

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
Y A	JP 2011-232475 A（三菱電機株式会社）2011.11.17, 段落【００２３】－【００２７】,【００３９】－【００４０】,【００５０】－【００７３】,【００８１】－【０１０６】,【０１５５】－【０１６４】,【図１】－【図２】,【図５】－【図１５】 & US 2013/0028415 A1 & EP 2565862 A1 & WO 2011/135895 A1 & CN 102859571 A & KR 10-2012-0139753 A	１，１１－１３ ２－１０

☑　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矛盾するものではなく、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	国際調査報告の発送日
０２．０８．２０１３	１３．０８．２０１３

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３１４６
松平　英
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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
Ｙ Ａ	Tatsuaki Okamoto et al, Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, [online], 2011.12.22, ［平成２５年８月２日検索］, インターネット＜URL:https://eprint.iacr.org/2010/563＞	１，１１－１３ ２－１０
Ｙ Ａ	Rosario Gennaro et al, Quadratic Span Programs and Succinct NIZKs without PCPs, [online], 2012.06.18, ［平成２５年８月２日検索］, インターネット<URL:https://eprint.iacr.org/2012/215>	１，１１－１３ ２－１０