(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
2012 年 8 月 16 日(16.08.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/108100 A1

(51) 国際特許分類:
H04L 9/30 (2006.01) *G09C 1/00* (2006.01)

(21) 国際出願番号: PCT/JP2011/078668

(22) 国際出願日: 2011 年 12 月 12 日(12.12.2011)

(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 2011-026216 2011 年 2 月 9 日(09.02.2011) JP

(71) 出願人 (米国を除く全ての指定国について): 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; および

(75) 発明者/出願人 (米国についてのみ): 高島 克幸(TAKASHIMA, Katsuyuki) [—/JP]; 〒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) [—/JP]; 〒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, 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, KM, 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, 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.

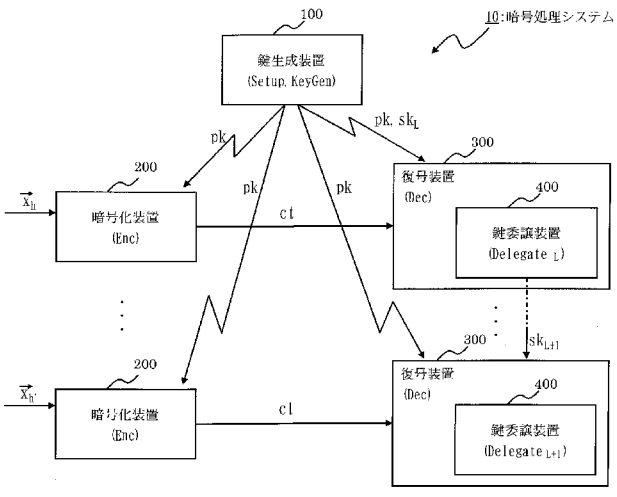
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,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

[続葉有]

(54) **Title**: ENCRYPTION PROCESSING SYSTEM, KEY GENERATION DEVICE, ENCRYPTION DEVICE, DECRYPTION DEVICE, KEY DELEGATION DEVICE, ENCRYPTION PROCESSING METHOD, AND ENCRYPTION PROCESSING PROGRAM

(54) 発明の名称 : 暗号処理システム、鍵生成装置、暗号化装置、復号装置、鍵委譲装置、暗号処理方法及び暗号処理プログラム

[図7]



200 Encryption device (Enc)
100 Key generation device (Setup, KeyGen)
10 Encryption processing system
300 Decryption device (Dec)
400 Key delegation device (Delegate $_L$)
400 Key delegation device (Delegate $_{L+1}$)

(57) **Abstract**: The purpose of the present invention is to provide hierarchical predicate encryption for inner products that achieves improved efficiency of a computation and the like. An encryption processing system (10) is provided with a key generation device (100), an encryption device (200), and a decryption device (300). The key generation device (100) generates, as a decryption key (sk_L), a vector in which predicate information ($v^{\rightarrow}_t$) is embedded in the basis vectors of a basis (B^*_t) regarding respective integers (t) of t=1, …, L. The encryption device (200) generates, as encrypted data (ct), a vector in which attribute information ($x^{\rightarrow}_t$) is embedded in the basis vectors of a basis (B_t) regarding at least some integers (t) among t=1, …, L. The decryption device (300) performs a pairing computation on the decryption key (sk_L) generated by the key generation device (100) and the encrypted data (ct) generated by the encryption device (200) to decrypt the encrypted data (ct).

(57) 要約:

[続葉有]

WO 2012/108100 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

演算等の効率をよくした階層的内積述語暗号を提供することを目的とする。暗号処理システム１０は、鍵生成装置１００と暗号化装置２００と復号装置３００とを備える。鍵生成装置１００は、ｔ＝１，．．．，Ｌの各整数ｔについての基底B^*_tの基底ベクトルに述語情報v_tを埋め込んだベクトルを復号鍵sk_Lとして生成する。暗号化装置２００は、ｔ＝１，．．．．，Ｌのうち少なくとも一部の整数ｔについての基底B_tの基底ベクトルに属性情報x_tを埋め込んだベクトルを暗号化データｃｔとして生成する。復号装置３００は、鍵生成装置１００が生成した復号鍵sk_Lと暗号化装置２００が生成した暗号化データｃｔとについてペアリング演算を行い、暗号化データｃｔを復号する。

明　細　書

発明の名称 ：

暗号処理システム、鍵生成装置、暗号化装置、復号装置、鍵委譲装置、暗号処理方法及び暗号処理プログラム

技術分野

[0001] この発明は、階層的述語暗号（Ｈｉｅｒａｒｃｈｉｃａｌ　Ｐｒｅｄｉｃａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ）に関するものである。

背景技術

[0002] 非特許文献２１には、階層的内積述語暗号（Ｈｉｅｒａｒｃｈｉｃａｌ　Ｐｒｅｄｉｃａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　ｆｏｒ　Ｉｎｎｅｒ　Ｐｒｏｄｕｃｔｓ）についての記載がある。また、非特許文献１８には、関数型暗号（Ｆｕｎｃｔｉｏｎａｌ　Ｅｎｃｒｙｐｔｉｏｎ）についての記載がある。

先行技術文献

非特許文献

[0003] 非特許文献1：Ｂｅｉｍｅｌ，　Ａ．，　Ｓｅｃｕｒｅ　ｓｃｈｅｍｅｓ　ｆｏｒ　ｓｅｃｒｅｔ　ｓｈａｒｉｎｇ　ａｎｄ　ｋｅｙ　ｄｉｓｔｒｉｂｕｔｉｏｎ．　ＰｈＤ　Ｔｈｅｓｉｓ，　Ｉｓｒａｅｌ　Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｔｅｃｈｎｏｌｏｇｙ，　Ｔｅｃｈｎｉｏｎ，　Ｈａｉｆａ，　Ｉｓｒａｅｌ，　１９９６．

非特許文献2：Ｂｅｔｈｅｎｃｏｕｒｔ，　Ｊ．，　Ｓａｈａｉ，　Ａ．，　Ｗａｔｅｒｓ，　Ｂ．：　Ｃｉｐｈｅｒｔｅｘｔ－ｐｏｌｉｃｙ　ａｔｔｒｉｂｕｔｅ－ｂａｓｅｄ　ｅｎｃｒｙｐｔｉｏｎ．　Ｉｎ：２００７　ＩＥＥＥ　Ｓｙｍｐｏｓｉｕｍ　ｏｎ　Ｓｅｃｕｒｉｔｙ　ａｎｄ　Ｐｒｉｖａｃｙ，　ｐｐ．　３２１･３４．　ＩＥＥＥ　Ｐｒｅｓｓ　（２００７）

非特許文献3：Ｂｏｎｅｈ，　Ｄ．，　Ｂｏｙｅｎ，　Ｘ．：　Ｅｆｆｉｃｉｅｎｔ　ｓｅｌｅｃｔｉｖｅ－ＩＤ　ｓｅｃｕｒｅ　ｉｄｅｎｔｉｔｙ　ｂ

ased encryption without random oracles. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-38. Springer Heidelberg (2004)

非特許文献4：Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In:Franklin, M. K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443-59. Springer Heidelberg (2004)

非特許文献5：Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440-56. Springer Heidelberg (2005)

非特許文献6：Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-29. Springer Heidelberg (2001)

非特許文献7：Boneh, D., Hamburg, M.: Generalized identity based and broadcast encryption scheme. In:Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455-70. Springer Heidelberg (2008)

非特許文献8：Boneh, D., Katz, J., Improved efficiency for CCA-secure cryptosystems built using identity based encryption. RSA-CT 2005, LNCS, Springer Verlag (2005)

非特許文献9：Boneh, D., Waters, B.：Conjunctive, subset, and range queries on encrypted data. In:Vadhan, S. P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535･54. Springer Heidelberg (2007)

非特許文献10：Boyen, X., Waters, B.：Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290･07. Springer Heidelberg (2006)

非特許文献11：Canetti, R., Halevi S., Katz J.：Chosen-ciphertext security from identity-based encryption. EUROCRYPT 2004, LNCS, Springer-Verlag (2004)

非特許文献12：Cocks, C.：An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) IMA Int. Conf. LNCS, vol. 2260, pp. 360･63. Springer Heidelberg (2001)

非特許文献13：Gentry, C.：Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445-64. Springer Heidelberg (2006)

非特許文献14：Gentry, C., Halevi, S.：Hierarchical identity-based encryption with polynomially many levels. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 437-56. Springer Heidelberg (2009)

非特許文献15：Gentry, C., Silverberg, A.：Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548-66. Springer Heidelberg (2002)

非特許文献16：Goyal, V., Pandey, O., Sahai, A., Waters, B.：Attribute-based encryption for fine-grained access control of encrypted data. In: ACM Conference on Computer and Communication Security 2006, pp. 89-8, ACM (2006)

非特許文献17：Katz, J., Sahai, A., Waters, B.：Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smar

t, N. P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146-62. Springer Heidelberg (2008)

非特許文献18：Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functionalencryption: Attribute-based encryption and (hierarchical) inner product encryption, EUROCRYPT 2010. LNCS, Springer Heidelberg (2010)

非特許文献19：Lewko, A. B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455-79. Springer Heidelberg (2010)

非特許文献20：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. 57-4. Springer Heidelberg (2008)

非特許文献21：Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products, In:ASIACRYPT 2009, Springer Heidelberg (2009)

非特許文献22：Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: ACM Conference on Computer and Communication Security 2007, pp. 195-03, ACM (2007)

非特許文献23：Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. In:ACM Conference on Computer and Communication Security 2006, pp. 99-12, ACM, (2006)

非特許文献24：Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 494, pp. 457-73. Springer Heidelberg (2005)

非特許文献25：Shi, E., Waters, B.: Delegating capability in predicate encryption systems. In: Aceto, L., Damg「エard, I., Goldberg, L.A., Halldウエrsson, M.M., Ingウエlfsdウエttir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, pp. 560.578. Springer Heidelberg (2008)

非特許文献26：Waters, B.: Efficient identity based encryption without random oracles. Eurocrypt 2005, LNCS, vo

l. 3152, pp. 443・59. Springer Verlag, (2005)

非特許文献27：Waters, B.: Ciphertext−policy attribute−based encryption: an expressive, efficient, and provably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290

非特許文献28：Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619・36. Springer Heidelberg (2009)

発明の概要

発明が解決しようとする課題

[0004] 非特許文献２１に記載された階層的内積述語暗号方式では、１つの大きな空間を使って暗号処理を構築していた。そのため、この階層的内積述語暗号方式を実装した場合、鍵のサイズが大きくなり、演算等の効率が悪くなる虞がある。

この発明は、演算等の効率をよくした階層的内積述語暗号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

[0005] この発明に係る暗号処理システムは、

ｔ＝１，．．．，Ｌ＋１（Ｌは１以上の整数）の各整数ｔについての基底B_tと基底B^*_tとを用いて暗号処理を行う暗号処理システムであり、

ｔ＝１，．．．，Ｌのうち少なくとも一部の整数ｔについての基底B_tの基底ベクトルに属性情報$\vec{x}_t$を埋め込んだベクトルを暗号化データｃｔとして生成する暗号化装置と、

ｔ＝１，．．．，Ｌの各整数ｔについての基底Ｂ＊$_t$の基底ベクトルに述語情報ｖ→$_t$を埋め込んだベクトルを復号鍵ｓｋ$_L$として、前記暗号化装置が生成した暗号化データｃｔと前記復号鍵ｓｋ$_L$とについてペアリング演算を行い前記暗号化データｃｔを復号する復号装置と、

基底Ｂ＊$_{L+1}$の基底ベクトルに述語情報を埋め込んだベクトルと、前記復号装置が使用した復号鍵ｓｋ$_L$とに基づき、前記復号鍵ｓｋ$_L$の下位の復号鍵ｓｋ$_{L+1}$を生成する鍵委譲装置と

を備えることを特徴とする。

発明の効果

[0006] この発明に係る暗号処理システムでは、複数の空間を用いて階層構造を構築している。そのため、鍵のサイズを小さくでき、演算効率がよくなる。

図面の簡単な説明

[0007] [図1]「権限委譲（階層的な権限委譲）」という概念を説明するための図。

[図2]階層を飛ばした権限委譲を説明するための図。

[図3]属性情報と述語情報との階層構造を示す図。

[図4]階層的ＩＤベース暗号の例を示す図。

[図5]基底と基底ベクトルとを説明するための図。

[図6]ベクトル空間における階層構造の実現方法の一例を説明するための図。

[図7]階層的内積述語暗号方式のアルゴリズムを実行する暗号処理システム１０の構成図。

[図8]鍵生成装置１００の機能を示す機能ブロック図。

[図9]暗号化装置２００の機能を示す機能ブロック図。

[図10]復号装置３００の機能を示す機能ブロック図。

[図11]鍵委譲装置４００の機能を示す機能ブロック図。

[図12]Ｓｅｔｕｐアルゴリズムの処理を示すフローチャート。

[図13]ＫｅｙＧｅｎアルゴリズムの処理を示すフローチャート。

[図14]Ｅｎｃアルゴリズムの処理を示すフローチャート。

[図15]Ｄｅｃアルゴリズムの処理を示すフローチャート。

[図16]Ｄｅｌｅｇａｔｅ$_L$アルゴリズムの処理を示すフローチャート。

[図17]ＫｅｙＧｅｎアルゴリズムの処理を示すフローチャート。

[図18]Ｄｅｃアルゴリズムの処理を示すフローチャート。

[図19]Ｄｅｌｅｇａｔｅ$_L$アルゴリズムの処理を示すフローチャート。

[図20]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

[0008] 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。出力装置は後述するＲＡＭ９１４、磁気ディスク９２０、通信ボード９１５、ＬＣＤ９０１等である。つまり、処理装置、記憶装置、通信装置、入力装置、出力装置はハードウェアである。

[0009] 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、

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

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。

数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。

[数110]

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

[数111]

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

$\vec{e}_{t,j}$は、数１１２に示す正規基底ベクトルを示す。

[数112]

$$\vec{e}_{t,j} : (\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n_t - j}) \in \mathbb{F}_q^{n_t} \ \text{for} \ j = 1, \ldots, n_t$$

また、数１１３から数１１７である。

[数113]

$$((\vec{x}_0)_{\mathbb{B}_0^*}, \ldots, (\vec{x}_d)_{\mathbb{B}_d^*}) + ((\vec{y}_0)_{\mathbb{B}_0^*}, \ldots, (\vec{y}_d)_{\mathbb{B}_d^*})$$
$$:= ((\vec{x}_0 + \vec{y}_0)_{\mathbb{B}_0^*}, \ldots, (\vec{x}_d + \vec{y}_d)_{\mathbb{B}_d^*})$$

[数114]

$$(\vec{x})_{\mathbb{B}_t^*} := ((\vec{0})_{\mathbb{B}_0^*},\ldots,\ (\vec{0})_{\mathbb{B}_{t-1}^*},(\vec{x})_{\mathbb{B}_t^*},(\vec{0})_{\mathbb{B}_{t+1}^*},\ldots,\ (\vec{0})_{\mathbb{B}_d^*})$$

[数115]

$$((\vec{x}_i)_{\mathbb{B}_i^*},\ (\vec{x}_j)_{\mathbb{B}_j^*}) := ((\vec{x}_i)_{\mathbb{B}_i^*} + (\vec{x}_j)_{\mathbb{B}_j^*}$$

[数116]

$$((\vec{x}_0)_{\mathbb{B}_0^*},(\vec{x}_t)_{\mathbb{B}_t^*};t=1,\ldots,L) := ((\vec{x}_0)_{\mathbb{B}_0^*},\ldots,\ (\vec{x}_L)_{\mathbb{B}_L^*})$$

[数117]

$$e(c,k^*) := \prod_{t=0}^{d} e(c_t,k_t^*),$$
$$\text{where } c := (c_0 \in \langle \mathbb{B}_0 \rangle,\ldots,c_d \in \langle \mathbb{B}_d \rangle),$$
$$k^* := (k_{L,0}^* \in \langle \mathbb{B}_0^* \rangle,\ldots,k_d^* \in \langle \mathbb{B}_d^* \rangle)$$

また、数１１８である場合に、数１１９である。

[数118]

$$k^* := ((\vec{x}_0)_{\mathbb{B}_0^*},\ldots,(\vec{x}_d)_{\mathbb{B}_d^*})$$

[数119]

$$[k^*]^L := ((\vec{x}_0)_{\mathbb{B}_0^*},\ldots,(\vec{x}_L)_{\mathbb{B}_L^*},(\vec{0})_{\mathbb{B}_{L+1}^*},\ldots,(\vec{0})_{\mathbb{B}_d^*}),$$
$$[k^*]_L := ((\vec{0})_{\mathbb{B}_0^*},\ldots,(\vec{0})_{\mathbb{B}_L^*},(\vec{x}_{L+1})_{\mathbb{B}_{L+1}^*},\ldots,(\vec{x}_d)_{\mathbb{B}_d^*})$$

[0010] また、以下の説明において、$F_{q^{nt}}$におけるntはn_tのことである。

同様に、秘密鍵$sk_{(v\to 1,\ldots,v\to L)}$における（$v\to 1$，．．．，$v\to L$）は（$\vec{v}_1$，．．．，$\vec{v}_L$）のことであり、秘密鍵$sk_{(v\to 1,\ldots,v\to L+1)}$における（$v\to 1$，．．．，$v\to L+1$）は（$\vec{v}_1$，．．．，$\vec{v}_{L+1}$）のこと

である。

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。

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。

[0011] また、以下の説明において、暗号処理とは、暗号化処理、復号処理、鍵生成処理、鍵委譲処理を含むものである。

[0012] 実施の形態１．

この実施の形態では、「階層的内積述語暗号」を実現する基礎となる概念と、「階層的内積述語暗号」の構成について説明する。

第１に、階層的内積述語暗号の概念について説明する。階層的内積述語暗号という概念を説明するに当たり、まず「権限委譲」という概念を説明する。また、併せて、「階層的（Ｈｉｅｒａｒｃｈｉａｌ）な権限委譲」という概念を説明する。次に、「内積述語暗号」を説明する。そして、階層的な権限委譲という概念を内積述語暗号に加えた「階層的内積述語暗号」を説明する。さらに、階層的内積述語暗号の理解を深めるため、階層的内積述語暗号の応用例を説明する。

第２に、ベクトル空間における階層的内積述語暗号を説明する。この実施の形態及び以下の実施の形態では、階層的述語暗号と階層的述語鍵秘匿方式とをベクトル空間において実現する。ここでは、まず、「基底」と「基底ベクトル」について説明する。次に、「ベクトル空間における内積述語暗号」について説明する。そして、「ベクトル空間における階層構造の実現方法」について説明する。さらに、理解を深めるため、階層構造の実現例を説明する。

第３に、階層的内積述語暗号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４に、この実施の形態に係る「階層的内積述語暗号方式」の基本構成を説明する。次に、階層的述語暗号を実行する「暗号処理システム１０」の基本構成を説明する。そして、この実施の形態に係る階層的述語暗号方式及び暗号処理システム１０について詳細に説明する。

[0013] ＜第１．階層的内積述語暗号＞

＜第１－１．権限委譲（階層的な権限委譲）という概念＞

図１は、「権限委譲（階層的な権限委譲）」という概念を説明するための図である。

権限委譲とは、上位の鍵を有する利用者が、その鍵（上位の鍵）よりも機能が制限された下位の鍵を生成することである。

図１では、Ｒｏｏｔ（鍵生成装置）は、マスター秘密鍵を用いて、第１層目（Ｌｅｖｅｌ－１）の利用者へ秘密鍵を生成する。つまり、Ｒｏｏｔは、第１層目の利用者１，２，３それぞれへ鍵１，２，３を生成する。そして、例えば、利用者１であれば、鍵１を用いて、利用者１の下位（第２層目）の利用者である利用者１１，１２，１３それぞれへ鍵１１，１２，１３を生成することができる。ここで、利用者１が有する鍵１よりも、利用者１１，１２，１３が有する鍵１１，１２，１３は機能が制限されている。機能が制限されているとは、その秘密鍵によって復号できる暗号文が限定されているということである。つまり、上位の秘密鍵で復号できる暗号文の一部の暗号文のみ下位の秘密鍵で復号できることを意味する。すなわち、利用者１が有する鍵１で復号できる暗号文のうち、一部の暗号文のみ利用者１１，１２，１３が有する鍵１１，１２，１３で復号することができる。また、通常は、鍵１１と鍵１２と鍵１３とが復号できる暗号文は異なる。一方、鍵１１と鍵１２と鍵１３が復号できる暗号文は、鍵１で復号することができる。

また、図１に示すように、各秘密鍵が階層（レベル）分けされていることを「階層的」という。つまり、図１に示すように、階層的に下位の鍵を生成することを「階層的な権限委譲」と呼ぶ。

[0014] なお、図１では、Ｒｏｏｔが第１層目の利用者へ秘密鍵を生成し、第１層

目の利用者が第２層目の利用者へ秘密鍵を生成し、第２層目の利用者が第３層目の利用者へ秘密鍵を生成すると説明した。しかし、図２に示すように、Ｒｏｏｔは、第１層目の利用者へ秘密鍵を生成するだけでなく、第２層目以下の層の利用者へ秘密鍵を生成することもできる。同様に、第１層目の利用者は、第２層目の利用者へ秘密鍵を生成するだけでなく、第３層目以下の層の利用者へ秘密鍵を生成することもできる。つまり、Ｒｏｏｔや利用者は、自分が持つ秘密鍵よりも下位の層の秘密鍵を生成することができる。

[0015] ＜第１－２．内積述語暗号＞

次に、「内積述語暗号」について説明する。

まず、述語暗号とは、述語情報f_vに属性情報ｘを入力した場合に１（Ｔｒｕｅ）となる場合（$f_v(x)=1$となる場合）に、暗号文を復号できる暗号方式である。通常、暗号文に属性情報ｘが埋め込まれ、秘密鍵に述語情報f_vが埋め込まれる。つまり、述語暗号では、属性情報ｘに基づき暗号化された暗号文ｃを、述語情報f_vに基づき生成された秘密鍵SK_fにより復号する。述語暗号は、例えば、述語情報f_vが条件式であり、属性情報ｘがその条件式への入力情報であり、入力情報（属性情報ｘ）が条件式（述語情報f_v）を満たせば（$f_v(x)=1$）、暗号文を復号できる暗号方式であるとも言える。

なお、述語暗号について詳しくは非特許文献１７に記載されている。

[0016] 内積述語暗号とは、属性情報ｘと述語情報f_vとの内積が所定の値の場合に、$f_v(x)=1$となる述語暗号である。つまり、属性情報ｘと述語情報f_vとの内積が所定の値の場合にのみ、属性情報ｘにより暗号化された暗号文ｃを、述語情報f_vに基づき生成された秘密鍵SK_fにより復号することができる。

実施の形態１では、原則として、属性情報ｘと述語情報f_vとの内積が０の場合に、$f_v(x)=1$となるものとする。

[0017] ＜第１－３．階層的内積述語暗号＞

階層的内積述語暗号（階層的内積述語鍵秘匿方式）とは、上述した「階層的な権限委譲」という概念を有する「内積述語暗号」である。

[0018] 階層的内積述語暗号は、内積述語暗号に階層的な権限委譲システムを持たせるため、属性情報と述語情報とに階層構造を持たせる。

図３は、属性情報と述語情報との階層構造を示す図である。

図３において、符号が対応する属性情報と述語情報とは対応する（つまり、内積が０となる）ものとする。つまり、属性１と述語１との内積は０となり、属性１１と述語１１との内積は０となり、属性１２と述語１２との内積は０となり、属性１３と述語１３との内積は０となるとする。すなわち、属性１により暗号化された暗号文ｃ１は、述語１に基づき生成された秘密鍵ｋ１であれば復号できる。また、属性１１により暗号化された暗号文ｃ１１は、述語１１に基づき生成された秘密鍵ｋ１１であれば復号できる。属性１２と述語１２、属性１３と述語１３についても同様のことが言える。

上記の通り、階層的内積述語暗号は階層的な権限委譲システムを有する。そのため、述語１に基づき生成された秘密鍵ｋ１と、述語１１とに基づき、秘密鍵ｋ１１を生成することができる。つまり、上位の秘密鍵ｋ１を有する利用者は、その秘密鍵ｋ１と下位の述語１１とから、秘密鍵ｋ１の下位の秘密鍵ｋ１１を生成することができる。同様に、秘密鍵ｋ１と述語１２とから秘密鍵ｋ１２を生成でき、秘密鍵ｋ１と述語１３とから秘密鍵ｋ１３を生成できる。

また、下位の秘密鍵に対応する鍵（公開鍵）で暗号化された暗号文を上位の秘密鍵で復号できる。一方、上位の秘密鍵に対応する鍵（公開鍵）で暗号化された暗号文は、下位の秘密鍵で復号できない。つまり、属性１１、属性１２、属性１３により暗号化された暗号文ｃ１１、ｃ１２、ｃ１３は、述語１に基づき生成された秘密鍵ｋ１であれば復号できる。一方、属性１により暗号化された暗号文ｃ１は、述語１１、述語１２、述語１３に基づき生成された秘密鍵ｋ１１、ｋ１２、ｋ１３では復号できない。すなわち、属性１１、属性１２、属性１３と述語１との内積は０となる。一方、属性１と述語１１、述語１２、述語１３との内積は０とならない。

[0019] ＜第１－４．階層的内積述語暗号の応用例＞

図４は、後述する階層的内積述語暗号の応用例である階層的ＩＤベース暗号（Ｈｉｅｒａｒｃｈｉａｌ　Ｉｄｅｎｔｉｆｉｅｒ　Ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ，ＨＩＢＥ）の例を示す図である。なお、階層的ＩＤベース暗号とは、ＩＤベース暗号が階層的になった暗号処理である。ＩＤベース暗号は、述語暗号の一種であり、暗号文に含まれるＩＤと秘密鍵に含まれるＩＤとが一致する場合に暗号文を復号できるマッチング述語暗号である。

図４に示す例では、Ｒｏｏｔ（鍵生成装置）は、マスター秘密鍵ｓｋとＡ会社のＩＤである「Ａ」とに基づき、ＩＤ「Ａ」に対応する秘密鍵（鍵Ａ）を生成する。例えば、Ａ会社のセキュリティ担当者は、鍵Ａと各部門のＩＤとに基づき、そのＩＤに対応する秘密鍵を生成する。例えば、セキュリティ担当者は、営業部門のＩＤである「Ａ－１」に対応する秘密鍵（鍵１）を生成する。次に、例えば、各部門の管理者は、その部門の秘密鍵とその部門に属する各課のＩＤとに基づき、そのＩＤに対応する秘密鍵を生成する。例えば、営業部門の管理者は、営業１課のＩＤである「Ａ－１１」に対応する秘密鍵（鍵１１）を生成する。

ここで、営業１課のＩＤ「Ａ－１１」に対応する秘密鍵である鍵１１により、営業１課のＩＤ「Ａ－１１」で暗号化された暗号文を復号することができる。しかし、鍵１１により、営業２課や営業３課のＩＤで暗号化された暗号文は復号することはできない。また、鍵１１により、営業部門のＩＤで暗号化された暗号文は復号することができない。

営業部門のＩＤ「Ａ－１」に対応する秘密鍵である鍵１により、営業部門のＩＤ「Ａ－１」で暗号化された暗号文を復号することができる。また、鍵１により、営業部門に属する課のＩＤで暗号化された暗号文を復号することができる。つまり、鍵１により、営業１課、営業２課、営業３課のＩＤで暗号化された暗号文を復号することができる。しかし、鍵１により、製造部門（ＩＤ：Ａ－２）やスタッフ部門（ＩＤ：Ａ－３）のＩＤで暗号化された暗号文は復号することができない。また、鍵１により、Ａ会社のＩＤで暗号化された暗号文は復号することができない。

Ａ会社のＩＤ「Ａ」に対応する秘密鍵である鍵Ａにより、Ａ会社のＩＤ「Ａ」で暗号化された暗号文を復号することができる。また、Ａ会社に属する各部門や、その部門に属する課のＩＤで暗号化された暗号文を復号することができる。

[0020] 階層的内積述語暗号は、ＩＤベース暗号以外へも様々な応用が可能である。特に、以下に説明する暗号処理は、等号関係テストのクラスに限定されたものではないため、非常に多くの応用が可能である。例えば、内積述語暗号の一種である検索可能暗号等についても、階層毎に検索可能な範囲をＡＮＤ条件やＯＲ条件等の条件式を用いて限定する等、従来の権限委譲システムを有する述語暗号では実現できなかった応用が可能である。

つまり、後の実施の形態で説明する階層的述語鍵秘匿方式と階層的述語暗号とは、ＩＤベース暗号や検索可能暗号等へ幅広い応用が可能である。

[0021] ＜第２．ベクトル空間における階層的内積述語暗号＞

階層的述語鍵秘匿方式と階層的述語暗号とは、後述する双対ペアリングベクトル空間という高次元ベクトル空間において実現される。そこで、ベクトル空間における階層的内積述語暗号を説明する。

[0022] ＜第２－１．基底と基底ベクトル＞

まず、ベクトル空間の説明において使用する「基底」と「基底ベクトル」とについて簡単に説明する。

図５は、基底と基底ベクトルとを説明するための図である。

図５は、２次元ベクトル空間におけるベクトルｖを示す。ベクトルｖは、$c_1 a_1 + c_2 a_2$である。また、ベクトルｖは、$y_1 b_1 + y_2 b_2$である。ここで、a_1，a_2を基底Ａにおける基底ベクトルといい、基底Ａ：＝（a_1，a_2）と表す。また、b_1，b_2を基底Ｂにおける基底ベクトルといい、基底Ｂ：＝（b_1，b_2）と表す。また、c_1，c_2，y_1，y_2は、各基底ベクトルに対する係数である。図５では、２次元ベクトル空間であったため、各基底における基底ベクトルは２個であった。しかし、Ｎ次元ベクトル空間であれば、各基底における基底ベクトルはＮ個である。

[0023] ＜第２－２．ベクトル空間における内積述語暗号＞

次に、ベクトル空間における内積述語暗号を説明する。

上記の通り、内積述語暗号とは、属性情報ｘと述語情報ｆ$_v$との内積が所定の値（ここでは、０）の場合に、ｆ$_v$（ｘ）＝１となる述語暗号である。属性情報ｘと述語情報ｆ$_v$とがベクトルであった場合、つまり属性ベクトルｘ$^{\rightarrow}$と述語ベクトルｖ$^{\rightarrow}$とであった場合、内積述語は数１２０のように定義される。

[数120]

$$\vec{x}\cdot\vec{v}=\sum_{i=1}^{n}x_i v_i=0 \text{ であれば、 } f_{\vec{v}}(\vec{x})=1,$$

$$\vec{x}\cdot\vec{v}=\sum_{i=1}^{n}x_i v_i\neq 0 \text{ であれば、 } f_{\vec{v}}(\vec{x})=0$$

ここで、

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

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

である。

つまり、属性ベクトルｘ$^{\rightarrow}$と述語ベクトルｖ$^{\rightarrow}$との内積、つまり要素毎の内積の和が０である場合に、述語情報ｆ$_v$に属性情報ｘを入力した結果が１（Ｔｒｕｅ）となる。また、属性ベクトルｘ$^{\rightarrow}$と述語ベクトルｖ$^{\rightarrow}$との内積が０でない場合に、述語情報ｆ$_v$に属性情報ｘを入力した結果が０（Ｆａｌｓｅ）となる述語暗号である。

[0024] ＜第２－３．ベクトル空間における階層構造の実現方法＞

次に、ベクトル空間における階層構造の実現方法を説明する。

図６は、ベクトル空間における階層構造の実現方法の一例を説明するための図である。

ここではｄ個（ｄは１以上の整数）のベクトル空間を扱う。各ベクトル空間は、高次元（Ｎ$_t$次元（ｔ＝１，．．．，ｄ））ベクトル空間である。つまり、各ベクトル空間における所定の基底Ｃ$_t$（ｔ＝１，．．．，ｄ）には、基底ベクトルｃ$_i$（ｉ＝１，．．．，Ｎ$_t$）のＮ$_t$個の基底ベクトルが存在する。

そして、基底C_1を第１層目の属性情報や述語情報を設定するための空間とする。また、基底C_2を第２層目の属性情報や述語情報を設定するための空間とする。以下同様に、基底C_Lを第Ｌ層目の属性情報や述語情報を設定するための空間とする。したがって、ここでは、ｄ層の階層を表すことができる。

ここで、第Ｌ層目の秘密鍵は、基底C_Lを用いて第Ｌ層目の述語情報を設定するだけでなく、基底C_1から基底C_{L-1}を用いて第１層目から第Ｌ－１層目の述語情報を設定して生成される。つまり、下位の層の秘密鍵には、上位の層の秘密鍵に設定される述語情報も設定される。これにより、述語情報に階層構造を持たせる。そして、この述語情報に持たせた階層構造を利用して、内積述語暗号における権限委譲システムを構成する。

[0025] なお、以下の説明においては、ベクトル空間における階層的構造を示すために、階層情報$\vec{n}$：＝（ｄ；N_1，．．．，N_d）を用いる。ここで、ｄは、上述した階層の深さを表す値である。N_i（ｉ＝１，．．．，ｄ）は、各層ｉに割り当てられた空間の次元数、つまり基底ベクトルの数を表す値である。

[0026] ＜第２－４．階層構造の実現例＞

ここで、簡単な例を用いて階層構造を説明する。ここでは、３つの階層を備え、各階層に割り当てられた空間が２次元で構成された例を用いて説明する。つまり、$\vec{n}$：＝（ｄ；N_1，．．．，N_d）＝（３；２，２，２）である。

第１層目の述語ベクトル$\vec{v}_1$：＝（v_1，v_2）に基づき生成された第１層目の秘密鍵sk_1を有する利用者は、第１層目の秘密鍵sk_1と第２層目の述語ベクトル$\vec{v}_2$：＝（v_3，v_4）に基づき第２層目の秘密鍵sk_2を生成することができる。つまり、第２層目の秘密鍵sk_2は、述語ベクトル（$\vec{v}_1$，$\vec{v}_2$）に基づき生成される。同様に、第２層目の秘密鍵sk_2を有する利用者は、第２層目の秘密鍵sk_2と第３層目の述語ベクトル$\vec{v}_3$：＝（v_5，v_6）に基づき第３層目の秘密鍵sk_3を生成することができる。つまり、第３層目の秘密鍵sk_3は、述語ベクトル（$\vec{v}_1$，$\vec{v}_2$，$\vec{v}_3$）に基づき生成される。

第１層目の述語ベクトル$\vec{v}_1$に基づき生成された第１層目の秘密鍵sk_1は

、（$\vec{v}_1$，（０，０），（０，０））により生成された秘密鍵である。そのため、第１層目の秘密鍵sk_1は、属性ベクトル（$\vec{x}_1$，（＊，＊），（＊，＊））：＝（（x_1，x_2），（＊，＊），（＊，＊））により暗号化された暗号文を、$\vec{v}_1 \cdot \vec{x}_1 = 0$である場合には復号できる。なぜなら、（＊，＊）・（０，０）＝０であるためである。ここで、“＊”は、任意の値を示す。

同様に、第２層目の述語ベクトル（$\vec{v}_1$，$\vec{v}_2$）に基づき生成された第２層目の秘密鍵sk_2は、（$\vec{v}_1$，$\vec{v}_2$，（０，０））により生成された秘密鍵である。そのため、第２層目の秘密鍵sk_2は、属性ベクトル（$\vec{x}_1$，$\vec{x}_2$，（＊，＊））：＝（（x_1，x_2），（x_3，x_4），（＊，＊））により暗号化された暗号文を、$\vec{v}_1 \cdot \vec{x}_1 = 0$かつ$\vec{v}_2 \cdot \vec{x}_2 = 0$である場合には復号できる。

しかし、第２層目の秘密鍵sk_2は、第１層目の属性ベクトル$\vec{x}_1$：＝（x_1，x_2）（つまり、（$\vec{x}_1$，（＊，＊），（＊，＊））により暗号化された暗号文を復号することはできない。なぜなら、$\vec{v}_2$＝（０，０）でなければ、（＊，＊）・$\vec{v}_2 \neq 0$であり、$\vec{v}_2 \cdot \vec{x}_2 \neq 0$であるためである。そのため、第２層目の秘密鍵$sk_2$は、親である秘密鍵鍵$sk_2$よりも限定された能力のみを有していると言える。

[0027] ＜第３．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（Ｓｙｍｍｅｔｒｉｃ Ｂｉｌｉｎｅａｒ Ｐａｉｒｉｎｇ Ｇｒｏｕｐｓ）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、$g \neq 0 \in G$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）$e: G \times G \to G_T$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、$e(g, g) \neq 1$である。

以下の説明において、数１２１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。

[数121]

$$\mathcal{G}_{bpg}$$

[0028] 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１２２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１２３に示す通りである。

[数122]

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

[数123]

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

[0029] 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１２４によって定義される。

[数124]

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

ここで、

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

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

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。

[0030] 演算（２）：ディストーション写像

数１２５に示す空間Ｖにおける線形変換$\phi_{i,j}$は、数１２６を行うことができる。

[数125]

$\phi_{i,j}(a_j)=a_i$であり、

$k\neq j$なら、$\phi_{i,j}(a_k)=0$である。

[数126]

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

ここで、

$(g_1,\cdots g_N):=x$

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。

[0031] 以下の説明において、数１２７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λ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。

[数127]

$\mathcal{G}_{\mathrm{dpvs}}$

[0032] 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。

[0033] ＜第４．階層的述語暗号の構成と暗号処理システム１０＞

＜第４－１．階層的内積述語暗号の基本構成＞

階層的内積述語暗号方式の構成を簡単に説明する。

階層的内積述語暗号方式は、Ｓｅｔｕｐ、ＫｅｙＧｅｎ、Ｅｎｃ、Ｄｅｃ、$\mathrm{Delegate}_L$（Ｌ＝１，．．．，ｄ－１）の５つの確率的多項式時間アルゴリズムを備える。

（Ｓｅｔｕｐ）

Ｓｅｔｕｐアルゴリズムでは、セキュリティパラメータ1^{λ}と階層情報$\vec{n}:=(d;N_0,\ldots,N_d)$とが入力され、マスター公開鍵ｐｋとマスター秘密鍵ｓｋとが出力される。マスター秘密鍵ｓｋは最も上位の鍵である。

（ＫｅｙＧｅｎ）

ＫｅｙＧｅｎアルゴリズムでは、マスター公開鍵ｐｋとマスター秘密鍵ｓｋと述語ベクトル$(\vec{v}_1,\ldots,\vec{v}_L)$（１≦Ｌ≦ｄ）が入力され、第Ｌ層目の秘密鍵$sk_{(\vec{v}_1,\ldots,\vec{v}_L)}$が出力される。

（Ｅｎｃ）

Ｅｎｃアルゴリズムでは、マスター公開鍵ｐｋと属性ベクトル$(\vec{x}_1,\ldots,\vec{x}_h)$（１≦ｈ≦ｄ）と平文情報ｍとが入力され、暗号化データｃｔ（暗号文）が出力される。つまり、Ｅｎｃアルゴリズムでは、平文情報ｍを埋め込み、属性ベクトル$(\vec{x}_1,\ldots,\vec{x}_h)$により暗号化された暗号化データｃｔが出力される。

（Ｄｅｃ）

Ｄｅｃアルゴリズムでは、マスター公開鍵ｐｋと第Ｌ層目の秘密鍵$sk_{(\vec{v}_1,\ldots,\vec{v}_L)}$と暗号化データｃｔとが入力され、平文情報ｍ又は識別情報⊥が

出力される。識別情報⊥とは、復号に失敗したことを示す情報である。つまり、Ｄｅｃアルゴリズムでは、暗号化データｃｔを第Ｌ層目の秘密鍵で復号して、平文情報ｍを抽出する。また、復号に失敗した場合には識別情報⊥を出力する。

（$\mathrm{Delegate}_L$）

$\mathrm{Delegate}_L$では、マスター公開鍵ｐｋと第Ｌ層目の秘密鍵$sk_{(\vec{v}_1,\ldots,\vec{v}_L)}$と第Ｌ＋１層目の述語ベクトル$\vec{v}_{L+1}$（Ｌ＋１≦ｄ）とが入力され、第Ｌ＋１層目の秘密鍵$sk_{(\vec{v}_1,\ldots,\vec{v}_{L+1})}$が出力される。つまり、$\mathrm{Delegate}_L$アルゴリズムでは、下位の秘密鍵が出力される。

[0034] ＜第４－２．暗号処理システム１０＞

階層的内積述語暗号方式のアルゴリズムを実行する暗号処理システム１０について説明する。

図７は、階層的内積述語暗号方式のアルゴリズムを実行する暗号処理システム１０の構成図である。

暗号処理システム１０は、鍵生成装置１００、暗号化装置２００、復号装置３００、鍵委譲装置４００を備える。なお、ここでは、復号装置３００が、鍵委譲装置４００を備えるものとして説明するが、鍵委譲装置４００は、復号装置３００とは別に設けられていてもよい。

鍵生成装置１００は、セキュリティパラメータλと、階層情報$\vec{n}:=(d;N_0,\ldots,N_d)$とを入力としてＳｅｔｕｐアルゴリズムを実行して、マスター公開鍵ｐｋとマスター秘密鍵ｓｋとを生成する。そして、鍵生成装置１００は、生成したマスター公開鍵ｐｋを公開する。また、鍵生成装置１００は、マスター公開鍵ｐｋとマスター秘密鍵ｓｋと述語ベクトル$(\vec{v}_1,\ldots,\vec{v}_L)$（１≦Ｌ≦ｄ）とを入力としてＫｅｙＧｅｎアルゴリズムを実行して、第Ｌ層目の秘密鍵$sk_{(\vec{v}_1,\ldots,\vec{v}_L)}$を生成して第Ｌ層目の復号装置３００へ秘密裡に配布する。

暗号化装置２００は、マスター公開鍵ｐｋと属性ベクトル$(\vec{x}_1,\ldots,\vec{x}_h)$（１≦ｈ≦ｄ）と平文情報ｍとを入力としてＥｎｃアルゴリズムを

実行して、暗号化データｃｔを生成する。暗号化装置２００は、生成した暗号化データｃｔを復号装置３００へ送信する。

復号装置３００は、マスター公開鍵ｐｋと第Ｌ層目の秘密鍵$sk_{(v\rightarrow 1,\ldots,v\rightarrow L)}$と暗号化データｃｔとを入力としてＤｅｃアルゴリズムを実行して、平文情報ｍ又は識別情報⊥を出力する。

鍵委譲装置４００は、スター公開鍵ｐｋと第Ｌ層目の秘密鍵$sk_{(v\rightarrow 1,\ldots,v\rightarrow L)}$と第Ｌ＋１層目の述語ベクトル$v\rightarrow_{L+1}$（Ｌ＋１≦ｄ）とを入力として$Delegate_L$アルゴリズムを実行して、第Ｌ＋１層目の秘密鍵$sk_{(v\rightarrow 1,\ldots,v\rightarrow L+1)}$を生成して第Ｌ＋１層目の復号装置３００へ秘密裡に配布する。

[0035] ＜第４－３．階層的内積述語暗号方式及び暗号処理システム１０の詳細＞

図８から図１６に基づき、実施の形態１に係る階層的内積述語暗号方式、及び、階層的内積述語暗号方式を実行する暗号処理システム１０の機能と動作とについて説明する。

図８は、鍵生成装置１００の機能を示す機能ブロック図である。図９は、暗号化装置２００の機能を示す機能ブロック図である。図１０は、復号装置３００の機能を示す機能ブロック図である。図１１は、鍵委譲装置４００の機能を示す機能ブロック図である。

図１２と図１３とは、鍵生成装置１００の動作を示すフローチャートである。なお、図１２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１３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１４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１５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。図１６は、鍵委譲装置４００の動作を示すフローチャートであり、$Delegate_L$アルゴリズムの処理を示すフローチャートである。

[0036] なお、以下の説明において、添え字の「ｄｅｃ」は「ｄｅｃｒｙｐｔｉｏ

ｎ」の略であり、添え字に「ｄｅｃ」とあるものは、暗号化データの復号に用いられる復号要素である。また、添え字の「ｒａｎ」は「ｒａｎｄｏｍｉｚａｔｉｏｎ」の略であり、添え字に「ｒａｎ」とあるものは、下位の復号鍵の所定の基底ベクトルに対する係数をランダム化するためのランダム化要素である。また、添え字の「ｄｅｌ」は「ｄｅｌｅｇａｔｉｏｎ」の略であり、添え字に「ｄｅｌ」とあるものは、下位の復号鍵を生成するための委譲要素である。

[0037] 鍵生成装置１００の機能と動作とについて説明する。

図８に示すように、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（第１情報入力部）、復号鍵生成部１４０、鍵配布部１５０（復号鍵送信部）を備える。

また、復号鍵生成部１４０は、乱数生成部１４１、復号要素生成部１４２、ランダム化要素生成部１４３、委譲要素生成部１４４を備える。

[0038] まず、図１２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１２８を計算して、$ｐａｒａｍ_{ｎ→}$と、ｔ＝０，．．．，ｄの各整数ｔについて基底$Ｂ_{ｔ}$及び基底$Ｂ^{*}_{ｔ}$をランダムに生成する。

[数128]

(1) input

$$1^{\lambda}, \vec{n} := (d; \vec{n} := (d; n_1, ..., n_d, u_0, ..., u_d, w_0, ..., w_d, z_0, ..., z_d)),$$
$$N_0 := 1 + u_0 + 1 + w_0 + z_0;\ N_t := n_t + u_t + w_t + z_t (t = 1, ..., d)$$

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

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

t＝0,...，dの各tについて（4）から（8）の処理を実行する。

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

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

(6) $(\nu_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1}$

(7) $b_{t,i} := (\chi_{t,i,1}, \cdots, \chi_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \chi_{t,i,j} a_{t,j},$

$\mathbb{B}_t := (b_{t,1}, \ldots, b_{t,N_t})$

(8) $b_{t,i}^* := (\nu_{t,i,1}, \cdots, \nu_{t,i,N_t})_{\mathbb{A}_t} = \sum_{j=1}^{N_t} \nu_{t,i,j} a_{t,j},$

$\mathbb{B}_t^* := (b_{t,1}^*, \ldots, b_{t,N_t}^*)$

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

$\mathrm{param}_n^{\rightarrow} := (\{\mathrm{param}_{\mathbb{V}_t}\}_{t=0,...,d}, g_T)$

[0039] 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}）と、属性のフォーマット$n^{\rightarrow}$：＝（ｄ；n_1，．．．，n_d，u_0，．．．，u_d，w_0，．．．，w_d，z_0，．．．，z_d）とを入力する。ここで、ｄは１以上の整数である。ｔ＝１，．．．，ｄの各整数ｔについてn_tは１以上の整数である。ｔ＝０，．．．，ｄまでの各整数ｔについてu_t，w_t，z_tは１以上の整数である。また、マスター鍵生成部１１０は、N_0：＝１

＋u_0＋１＋w_0＋z_0とし、ｔ＝１，．．．．，ｄの各整数ｔについてN_t：＝n_t＋u_t＋w_t＋z_tとする。

（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（1^{λ}）を入力としてアルゴリズムG_{bpg}を実行して、ランダムに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。

[0040] 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（４）から（８）までの処理を実行する。

（４）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（1^{λ}）及び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。

（５）マスター鍵生成部１１０は、処理装置により、（３）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。

（６）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、$(\nu_{t,i,j})_{i,j}$：＝φ・$(X_t^T)^{-1}$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。

（７）マスター鍵生成部１１０は、処理装置により、（５）で生成した線形変換X_tに基づき、（４）で生成した標準基底A_tから基底B_tを生成する。

（８）マスター鍵生成部１１０は、処理装置により、（６）で生成した$(\nu_{t,i,j})_{i,j}$に基づき、（４）で生成した標準基底A_tから基底B^*_tを生成

する。

（９）マスター鍵生成部１１０は、処理装置により、g_Tにｅ（ｇ，ｇ）$^{\phi}$を設定する。また、マスター鍵生成部１１０は、$param_{\vec{n}}$に（４）で生成した$\{param_{V_t}\}_{t=0,\ldots,d}$と、$g_T$とを設定する。なお、ｔ＝０，．．．，ｄとｉ＝１，．．．，N_tとの各整数ｔ，ｉについて、$g_T=e(b_{t,i}, b^*_{t,i})$である。

[0041] すなわち、（Ｓ１０１）で、マスター鍵生成部１１０は、数１２９に示すアルゴリズムG_{ob}を実行して、$param_{\vec{n}}$と、ｔ＝０，．．．，ｄの各整数ｔについて基底B_t及び基底B^*_tとを生成する。

[数129]

$$
\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}:=(d;\vec{n}:=(d;n_1,...,n_d,u_0,...,u_d,w_0,...,w_d,z_0,...,z_d)):\\
&\quad N_0:=1+u_0+1+w_0+z_0,\ N_t:=n_t+u_t+w_t+z_t \quad \text{for } t=1,..,d,\\
&\quad \mathsf{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{R}\mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),\\
&\quad \psi\xleftarrow{U}\mathbb{F}_q^{\times},\\
&\quad \text{For } t=0,\ldots,d,\\
&\qquad \mathsf{param}_{\mathbb{V}_t}:=(q,\mathbb{V}_t,\mathbb{G}_T,\mathbb{A}_t,e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t,\mathsf{param}_{\mathbb{G}}),\\
&\qquad X_t:=(\chi_{t,i,j})_{i,j}\xleftarrow{U}GL(N_t,\mathbb{F}_q),\quad (\nu_{t,i,j})_{i,j}:=\psi\cdot(X_t^{\mathrm{T}})^{-1},\\
&\qquad b_{t,i}:=(\chi_{t,i,1},\cdots,\chi_{t,i,N_t})_{\mathbb{A}_t}=\sum_{j=1}^{N_t}\chi_{t,i,j}a_{t,j},\ \mathbb{B}_t:=(b_{t,1},\ldots,b_{t,N_t}),\\
&\qquad b^*_{t,i}:=(\nu_{t,i,1},\cdots,\nu_{t,i,N_t})_{\mathbb{A}_t}=\sum_{j=1}^{N_t}\nu_{t,i,j}a_{t,j},\quad \mathbb{B}^*_t:=(b^*_{t,1},\ldots,b^*_{t,N_t}),\\
&\quad g_T:=e(g,g)^{\psi},\quad \mathsf{param}^{-}_{\vec{n}}:=(\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,\ldots,d},g_T)\\
&\quad \text{return } (\mathsf{param}^{-}_{\vec{n}},\{\mathbb{B}_t,\mathbb{B}^*_t\}_{t=0,\ldots,d}).
\end{aligned}
$$

[0042] （Ｓ１０２：マスター公開鍵生成ステップ）

マスター鍵生成部１１０は、処理装置により、基底B_0の部分基底$B\hat{}_0$と、ｔ＝１，．．．，ｄの各整数ｔについて、基底B_tの部分基底$B\hat{}_t$を数１３０に示すように生成する。

[数130]

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+1}, b_{0,1+u_0+1+w_0+1}, \ldots, b_{0,1+u_0+1+w_0+z_0}),$$
$$\hat{\mathbb{B}}_t := (b_{t,1}, .., b_{t,n_t}, b_{t,n_t+u_t+w_t+1}, \ldots, b_{t,n_t+u_t+w_t+z_t}) \quad \text{for } t = 1, .., d$$

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（1^λ）と、（Ｓ１０１）で生成したｐａｒａｍ$_{n\to}$と、基底ベクトルｂ*$_{0,\,1+u0+1+1,\ldots,}$ｂ*$_{0,\,1+u0+1+w0}$（ここでｕ０、ｗ０は、ｕ$_0$，ｗ$_0$のことである）と、ｔ＝１，．．．，ｄの各整数ｔについて基底ベクトルｂ*$_{t,\,nt+ut+1}$，．．．，ｂ*$_{t,\,nt+ut+wt}$（ここでｎｔ，ｕｔ，ｗｔは、ｎ$_t$，ｕ$_t$，ｗ$_t$のことである）とを合わせて、マスター公開鍵ｐｋとする。

[0043] （Ｓ１０３：マスター秘密鍵生成ステップ）

マスター鍵生成部１１０は、処理装置により、基底Ｂ*$_0$の部分基底Ｂ＾*$_0$と、ｔ＝１，．．．，ｄの各整数ｔについて、基底Ｂ*$_t$の部分基底Ｂ＾*$_t$を数１３１に示すように生成する。

[数131]

$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,1+u_0+1}^*),$$
$$\hat{\mathbb{B}}_t^* := (b_{t,1}^*, .., b_{t,n_t}^*) \quad \text{for } t = 1, .., d$$

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＾*$_t$とをマスター秘密鍵とする。

[0044] （Ｓ１０４：マスター鍵記憶ステップ）

マスター鍵記憶部１２０は、（Ｓ１０２）で生成したマスター公開鍵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秘密鍵ｓｋを記憶装置に記憶する。

[0045] つまり、（Ｓ１０１）から（Ｓ１０３）において、鍵生成装置１００は数１３２に示すＳｅｔｕｐアルゴリズムを実行して、マスター公開鍵ｐｋとマスター秘密鍵ｓｋとを生成する。そして、（Ｓ１０４）で、鍵生成装置１０

０は生成された公開パラメータｐｋとマスター鍵ｓｋとを記憶装置に記憶する。

なお、マスター公開鍵ｐｋは、例えば、ネットワークを介して公開され、復号装置３００が取得可能な状態にされる。

[数132]

$$\begin{aligned}
&\mathsf{Setup}(1^{\lambda},\ \vec{n} := (d; n_1,...,n_d, u_0,...,u_d, w_0,...,w_d, z_0,...,z_d)):\\
&\quad (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,...,d}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n}),\\
&\quad \hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+1}, b_{0,1+u_0+1+w_0+1}, ..., b_{0,1+u_0+1+w_0+z_0}),\\
&\quad \hat{\mathbb{B}}_t := (b_{t,1}, .., b_{t,n_t}, b_{t,n_t+u_t+w_t+1}, ..., b_{t,n_t+u_t+w_t+z_t}) \quad \text{for } t = 1,..,d,\\
&\quad \hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,1+u_0+1}^*),\\
&\quad \hat{\mathbb{B}}_t^* := (b_{t,1}^*, .., b_{t,n_t}^*) \quad \text{for } t = 1,..,d,\\
&\quad \mathsf{pk} := (1^{\lambda}, \mathsf{param}_{\vec{n}}, \{\hat{\mathbb{B}}_t\}_{t=0,...,d},\\
&\qquad\quad b_{0,1+u_0+1+1}^*, ..., b_{0,1+u_0+1+w_0}^*, \{b_{t,n_t+u_t+1}^*, ..., b_{t,n_t+u_t+w_t}^*\}_{t=1,...,d}),\\
&\quad \mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,...,d},\\
&\quad \text{return } \mathsf{pk},\ \mathsf{sk}.
\end{aligned}$$

[0046] 次に、図１３に基づき、鍵生成装置１００が実行する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、述語情報（$v^{\rightarrow}_1$，．．．，$v^{\rightarrow}_L$）：＝（（$v_{1,i}$（ｉ＝１，．．．，n_1））），．．．，（$v_{L,i}$（ｉ＝１，．．．，n_L））））を入力する。なお、述語情報としては、鍵を使用する者の属性が入力される。

[0047] （Ｓ２０２：乱数生成ステップ）

乱数生成部１４１は、処理装置により、ｊ＝１，．．．，２Ｌと，τ＝Ｌ＋１，．．．，ｄと，（τ，ι）＝（τ，１），．．．，（τ，n_τ）との各整数ｊ，τ，ιについて、乱数φと、乱数$s_{dec,t}$，$s_{ran,j,t}$（ｔ＝１，．．．，Ｌ）と、乱数$\theta_{dec,t}$，$\theta_{ran,j,t}$，$\eta^{\rightarrow}_{dec,t}$，$\eta^{\rightarrow}_{ran,j,t}$（ｔ

＝０，．．．，Ｌ）と、乱数$s_{ran,(\tau,\iota),t}$，$s_{del,(\tau,\iota),t}$（ｔ＝１，．．．，Ｌ＋１）と、乱数$\theta_{ran,(\tau,\iota),t}$，$\theta_{del,(\tau,\iota),t}$，$\vec{\eta}_{ran,(\tau,\iota),t}$，$\vec{\eta}_{del,(\tau,\iota),t}$（ｔ＝０，．．．，Ｌ＋１）とを数１３３に示すように生成する。

[数133]

$$\text{for } j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$$
$$\psi,s_{\mathrm{dec},t},s_{\mathrm{ran},j,t}\xleftarrow{\mathrm{U}}\mathbb{F}_q\ (t=1,...,L),$$
$$\theta_{\mathrm{dec},t},\theta_{\mathrm{ran},j,t}\xleftarrow{\mathrm{U}}\mathbb{F}_q\ (t=0,...,L),$$
$$\vec{\eta}_{\mathrm{dec},t}:=(\eta_{\mathrm{dec},t,1},...,\eta_{\mathrm{dec},t,w_t})\xleftarrow{\mathrm{U}}\mathbb{F}_q^{w_t}\ (t=0,...,L),$$
$$\vec{\eta}_{\mathrm{ran},j,t}:=(\eta_{\mathrm{ran},j,t,1},...,\eta_{\mathrm{ran},j,t,w_t})\xleftarrow{\mathrm{U}}\mathbb{F}_q^{w_t}\ (t=0,...,L),$$
$$s_{\mathrm{ran},(\tau,\iota),t},s_{\mathrm{del},(\tau,\iota),t}\xleftarrow{\mathrm{U}}\mathbb{F}_q\ (t=1,...,L+1),$$
$$\theta_{\mathrm{ran},(\tau,\iota),t},\theta_{\mathrm{del},(\tau,\iota),t}\xleftarrow{\mathrm{U}}\mathbb{F}_q\ (t=0,...,L+1),$$
$$\vec{\eta}_{\mathrm{ran},(\tau,\iota),t}:=(\eta_{\mathrm{ran},(\tau,\iota),t,1},...,\eta_{\mathrm{ran},(\tau,\iota),t,w_t})\xleftarrow{\mathrm{U}}\mathbb{F}_q^{w_t}\ (t=0,...,L+1),$$
$$\vec{\eta}_{\mathrm{del},(\tau,\iota),t}:=(\eta_{\mathrm{del},(\tau,\iota),t,1},...,\eta_{\mathrm{del},(\tau,\iota),t,w_t})\xleftarrow{\mathrm{U}}\mathbb{F}_q^{w_t}\ (t=0,...,L+1)$$

また、数１３４に示すように$s_{dec,0}$と、$s_{ran,j,0}$と、$s_{ran,(\tau,\iota),0}$と、$s_{del,(\tau,\iota),0}$とを設定する。

[数134]

$$s_{\mathrm{dec},0}:=\sum_{t=1}^{L}s_{\mathrm{dec},t},$$
$$s_{\mathrm{ran},j,0}:=\sum_{t=1}^{L}s_{\mathrm{ran},j,t},$$
$$s_{\mathrm{ran},(\tau,\iota),0}:=\sum_{t=1}^{L+1}s_{\mathrm{ran},(\tau,\iota),t},$$
$$s_{\mathrm{del},(\tau,\iota),0}:=\sum_{t=1}^{L+1}s_{\mathrm{del},(\tau,\iota),t}$$

[0048] （Ｓ２０３：復号要素生成ステップ）

復号要素生成部１４２は、処理装置により、復号鍵ｓｋ$_L$の要素である復号要素ｋ*$_{L,dec}$を数１３５に示すように生成する。

[数135]

$$k^*_{L,\mathrm{dec}} := ((-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0}, \\ (s_{\mathrm{dec},t}\ \vec{e}_{t,1} + \theta_{\mathrm{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,...,L)$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１３５は、以下のように、基底Ｂ*$_0$及び基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の基底ベクトルの係数が設定され、復号要素ｋ*$_{L,dec}$が生成されることを意味する。

まず、基底Ｂ*$_0$の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*$_{0,1}$，．．．，ｂ*$_{0,3}$を意味する。

基底Ｂ*$_0$の基底ベクトル１の係数としてーｓ$_{dec,0}$が設定される。基底ベクトル１＋１，．．．，１＋ｕ$_0$の係数として０が設定される。基底ベクトル１＋ｕ$_0$＋１の係数として１が設定される。基底ベクトル１＋ｕ$_0$＋１＋１，．．．，１＋ｕ$_0$＋１＋ｗ$_0$の係数として$\eta_{dec,0,1}$，．．．，$\eta_{dec,0,wo}$（ここで、ｗ０はｗ$_0$のことである）が設定される。基底ベクトル１＋ｕ$_0$＋１＋ｗ$_0$＋１，．．．，１＋ｕ$_0$＋１＋ｗ$_0$＋ｚ$_0$の係数として０が設定される。

次に、基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*$_{t,1}$，．．．，ｂ*$_{t,3}$を意味する。

基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数としてｓ$_{dec,t}$＋$\theta_{dec,t}$ｖ$_{t,1}$が設定される。基底ベクトル２，．．．，ｎ$_t$の係数として

$\theta_{dec,t}v_{t,2}$，．．．，$\theta_{dec,t}v_{t,nt}$（ここで、ｎｔはn_tのことである）が設定される。基底ベクトルn_t+1，．．．，n_t+u_tの係数として０が設定される。基底ベクトルn_t+u_t+1，．．．，$n_t+u_t+w_t$の係数として$\eta_{dec,t,1}$，．．．，$\eta_{dec,t,wt}$（ここで、ｗｔはw_tのことである）が設定される。基底ベクトル$n_t+u_t+w_t+1$，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

[0049] （Ｓ２０４：第１ランダム化要素生成ステップ）

ランダム化要素生成部１４３は、処理装置により、ｊ＝１，．．．，２Ｌの各整数ｊについて、復号鍵sk_Lの要素である第１ランダム化要素$k^*_{L,ran,j}$を数１３６に示すように生成する。

[数136]

$$k^*_{L,\mathrm{ran},j} := ((-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0}, \\ (s_{\mathrm{ran},j,t}\,\vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t} \\ : t = 1,\ldots,L)$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１３６は、以下のように、基底B^*_0及び基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトルの係数が設定され、第１ランダム化要素$k^*_{L,ran,j}$が生成されることを意味する。

まず、基底B^*_0の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{0,1}$，．．．，$b^*_{0,3}$を意味する。

基底B^*_0の基底ベクトル１の係数として$-s_{ran,j,0}$が設定される。基底ベクトル$1+1$，．．．，$1+u_0+1$の係数として０が設定される。基底ベクトル$1+u_0+1+1$，．．．，$1+u_0+1+w_0$の係数として$\eta_{ran,j,0,1}$，．．．，$\eta_{ran,j,0,wo}$（ここで、ｗ０はw_0のことである）が設定され

る。基底ベクトル１＋ｕ$_0$＋１＋ｗ$_0$＋１，．．．，１＋ｕ$_0$＋１＋ｗ$_0$＋ｚ$_0$の係数として０が設定される。

次に、基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*$_{t,1}$，．．．，ｂ*$_{t,3}$を意味する。

基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数としてｓ$_{ran,j,t}$＋$\theta_{ran,j,t}$ｖ$_{t,1}$が設定される。基底ベクトル２，．．．，ｎ$_t$の係数として$\theta_{ran,j,t}$ｖ$_{t,2}$，．．．，$\theta_{ran,j,t}$ｖ$_{t,nt}$（ここで、ｎｔはｎ$_t$のことである）が設定される。基底ベクトルｎ$_t$＋１，．．．，ｎ$_t$＋ｕ$_t$の係数として０が設定される。基底ベクトルｎ$_t$＋ｕ$_t$＋１，．．．，ｎ$_t$＋ｕ$_t$＋ｗ$_t$の係数として$\eta_{ran,j,t,1}$，．．．，$\eta_{ran,j,t,wt}$（ここで、ｗｔはｗ$_t$のことである）が設定される。基底ベクトルｎ$_t$＋ｕ$_t$＋ｗ$_t$＋１，．．．，ｎ$_t$＋ｕ$_t$＋ｗ$_t$＋ｚ$_t$の係数として０が設定される。

[0050] （Ｓ２０５：第２ランダム化要素生成ステップ）

ランダム化要素生成部１４３は、処理装置により、τ＝Ｌ＋１，．．．，ｄの各整数τと、各整数τについてι＝１，．．．，ｎ$_\tau$の各整数ιとについて、復号鍵ｓｋ$_L$の要素である第２ランダム化要素ｋ*$_{L,ran,(\tau,\iota)}$を数１３７に示すように生成する。

[数137]

$$
\begin{aligned}
k^*_{L,\mathrm{ran},(\tau,\iota)} \coloneqq (\ & (-s_{\mathrm{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0}, \\
& (s_{\mathrm{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t} \\
& : t = 1,\ldots,L \\
& (s_{\mathrm{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})
\end{aligned}
$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１３７は、以下のように、基底Ｂ*$_0$と基底Ｂ*$_t$

（ｔ＝１，．．．，Ｌ）と基底Ｂ*$_{\tau}$との基底ベクトルの係数が設定され、第２ランダム化要素ｋ*$_{L,\ ran,\ (\tau,\ \iota)}$が生成されることを意味する。

まず、基底Ｂ*$_{0}$の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{0,\ i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{0,\ 1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*$_{0,\ 1}$，．．．，ｂ*$_{0,\ 3}$を意味する。

基底Ｂ*$_{0}$の基底ベクトル１の係数として－ｓ$_{ran,\ (\tau,\ \iota),\ 0}$が設定される。基底ベクトル１＋１，．．．，１＋ｕ$_{0}$＋１の係数として０が設定される。基底ベクトル１＋ｕ$_{0}$＋１＋１，．．．，１＋ｕ$_{0}$＋１＋ｗ$_{0}$の係数として$\eta_{ran,\ (\tau,\ \iota),\ 0,\ 1}$，．．．，$\eta_{ran,\ (\tau,\ \iota),\ 0,\ wo}$（ここで、ｗ０はｗ$_{0}$のことである）が設定される。基底ベクトル１＋ｕ$_{0}$＋１＋ｗ$_{0}$＋１，．．．，１＋ｕ$_{0}$＋１＋ｗ$_{0}$＋ｚ$_{0}$の係数として０が設定される。

次に、基底Ｂ*$_{t}$（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{t,\ i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{t,\ 1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*$_{t,\ 1}$，．．．，ｂ*$_{t,\ 3}$を意味する。

基底Ｂ*$_{t}$（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数としてｓ$_{ran,\ (\tau,\ \iota),\ t}$＋$\theta_{ran,\ (\tau,\ \iota),\ t}$ｖ$_{t,\ 1}$が設定される。基底ベクトル２，．．．，ｎ$_{t}$の係数として$\theta_{ran,\ (\tau,\ \iota),\ t}$ｖ$_{t,\ 2}$，．．．，$\theta_{ran,\ (\tau,\ \iota),\ t}$ｖ$_{t,\ nt}$（ここで、ｎｔはｎ$_{t}$のことである）が設定される。基底ベクトルｎ$_{t}$＋１，．．．，ｎ$_{t}$＋ｕ$_{t}$の係数として０が設定される。基底ベクトルｎ$_{t}$＋ｕ$_{t}$＋１，．．．，ｎ$_{t}$＋ｕ$_{t}$＋ｗ$_{t}$の係数として$\eta_{ran,\ (\tau,\ \iota),\ t,\ 1}$，．．．，$\eta_{ran,\ (\tau,\ \iota),\ t,\ wt}$（ここで、ｗｔはｗ$_{t}$のことである）が設定される。基底ベクトルｎ$_{t}$＋ｕ$_{t}$＋ｗ$_{t}$＋１，．．．，ｎ$_{t}$＋ｕ$_{t}$＋ｗ$_{t}$＋ｚ$_{t}$の係数として０が設定される。

次に、基底Ｂ*$_{\tau}$の部分について説明する。ここでは、表記を簡略化して、

基底ベクトルｂ＊$_{\tau,\ i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ＊$_{\tau,\ 1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ＊$_{\tau,\ 1}$，．．．，ｂ＊$_{\tau,\ 3}$を意味する。

基底Ｂ＊$_{\tau}$の基底ベクトル１の係数としてｓ$_{ran,\ (\tau,\ \iota),\ L+1}$が設定される。基底ベクトル２，．．．，ｎ$_{\tau}$，．．．，ｎ$_{\tau}$＋ｕ$_{\tau}$の係数として０が設定される。基底ベクトルｎ$_{\tau}$＋ｕ$_{\tau}$＋１，．．．，ｎ$_{\tau}$＋ｕ$_{\tau}$＋ｗ$_{\tau}$の係数として$\eta_{ran,\ (\tau,\ \iota),\ L+1,\ 1}$，．．．，$\eta_{ran,\ (\tau,\ \iota),\ L+1,\ w\tau}$（ここで、ｗτはｗ$_{\tau}$のことである）が設定される。基底ベクトルｎ$_{\tau}$＋ｕ$_{\tau}$＋ｗ$_{\tau}$＋１，．．．，ｎ$_{\tau}$＋ｕ$_{\tau}$＋ｗ$_{\tau}$＋ｚ$_{\tau}$の係数として０が設定される。

[0051] （Ｓ２０６：委譲要素生成ステップ）

委譲要素生成部１４４は、処理装置により、τ＝Ｌ＋１，．．．，ｄの各整数τと、各整数τについてι＝１，．．．，ｎ$_{\tau}$の各整数ιとについて、復号鍵ｓｋ$_{L}$の要素である委譲要素ｋ＊$_{L,\ del,\ (\tau,\ \iota)}$を数１３８に示すように生成する。

[数138]

$$
\begin{aligned}
k^{*}_{L,\mathrm{del},(\tau,\iota)} := (\ & (-s_{\mathrm{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^{*}_{0}}, \\
& (s_{\mathrm{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{del},(\tau,\iota),t}\vec{v}_{t},\ 0^{u_t}, \vec{\eta}_{\mathrm{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^{*}_{t}} \\
& : t = 1,\ldots,L \\
& (s_{\mathrm{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^{*}_{\tau}})
\end{aligned}
$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ＊とに対して、数１１１である。したがって、数１３８は、以下のように、基底Ｂ＊$_{0}$と基底Ｂ＊$_{t}$（ｔ＝１，．．．，Ｌ）と基底Ｂ＊$_{\tau}$との基底ベクトルの係数が設定され、委譲要素ｋ＊$_{L,\ del,\ (\tau,\ \iota)}$が生成されることを意味する。

まず、基底Ｂ＊$_{0}$の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ＊$_{0,\ i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ＊$_{0,\ 1}$を意味する。また、基底

ベクトル１，．．．，３であれば、基底ベクトル$b^*_{0,1}$，．．．，$b^*_{0,3}$を意味する。

基底B^*_0の基底ベクトル１の係数として$-s_{del,(\tau,\iota),0}$が設定される。基底ベクトル１＋１，．．．，１＋u_0＋１の係数として０が設定される。基底ベクトル１＋u_0＋１＋１，．．．，１＋u_0＋１＋w_0の係数として$\eta_{del,(\tau,\iota),0,1}$，．．．，$\eta_{del,(\tau,\iota),0,wo}$（ここで、ｗ０は$w_0$のことである）が設定される。基底ベクトル１＋$u_0$＋１＋$w_0$＋１，．．．，１＋$u_0$＋１＋$w_0$＋$z_0$の係数として０が設定される。

次に、基底B^*_t（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{t,1}$，．．．，$b^*_{t,3}$を意味する。

基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数として$s_{del,(\tau,\iota),t}+\theta_{del,(\tau,\iota),t}v_{t,1}$が設定される。基底ベクトル２，．．．，$n_t$の係数として$\theta_{del,(\tau,\iota),t}v_{t,2}$，．．．，$\theta_{del,(\tau,\iota),t}v_{t,nt}$（ここで、ｎｔは$n_t$のことである）が設定される。基底ベクトル$n_t$＋１，．．．，$n_t$＋$u_t$の係数として０が設定される。基底ベクトル$n_t$＋$u_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$の係数として$\eta_{del,(\tau,\iota),t,1}$，．．．，$\eta_{del,(\tau,\iota),t,wt}$（ここで、ｗｔは$w_t$のことである）が設定される。基底ベクトル$n_t$＋$u_t$＋$w_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$＋$z_t$の係数として０が設定される。

次に、基底B^*_τの部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{\tau,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{\tau,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{\tau,1}$，．．．，$b^*_{\tau,3}$を意味する。

基底B^*_τの基底ベクトル１，．．．，n_τの係数として$s_{del,(\tau,\iota),L+1}$

$\vec{e}_{\tau,1}+\phi\vec{e}_{\tau,\iota}$が設定される。基底ベクトル$n_\tau+1,\ldots,n_\tau+u_\tau$の係数として０が設定される。基底ベクトル$n_\tau+u_\tau+1,\ldots,n_\tau+u_\tau+w_\tau$の係数として$\eta_{del,(\tau,\iota),L+1,1},\ldots,\eta_{del,(\tau,\iota),L+1,w\tau}$（ここで、$w\tau$は$w_\tau$のことである）が設定される。基底ベクトル$n_\tau+u_\tau+w_\tau+1,\ldots,n_\tau+u_\tau+w_\tau+z_\tau$の係数として０が設定される。

[0052] （Ｓ２０７：鍵配布ステップ）

鍵配布部１５０は、復号要素$k^*_{L,dec}$と、第１ランダム化要素$k^*_{L,ran,j}$（ｊ＝１，．．．，２Ｌ）と、第２ランダム化要素$k^*_{L,ran,(\tau,\iota)}$（τ＝Ｌ＋１，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，n_τ））と、委譲要素$k^*_{L,del,(\tau,\iota)}$（τ＝Ｌ＋１，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，n_τ））とを要素とする復号鍵sk_L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_Lは、他の方法により復号装置３００へ配布されてもよい。

[0053] つまり、（Ｓ２０１）から（Ｓ２０６）において、鍵生成装置１００は数１３９、数１４０に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵sk_Lを生成する。そして、（Ｓ２０７）で、鍵生成装置１００は生成された復号鍵sk_Lを復号装置３００へ配布する。

[数139]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,...,\vec{v}_L) := (v_{1,1},...,v_{1,n_1}),...,\ (v_{L,1},...,v_{L,n_L})):$$

for $j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (t=1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t}\ (t=0,...,L);$$

$$s_{\mathsf{ran},(\tau,\iota),t}, s_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q\ (t=1,...,L+1);$$

$$\theta_{\mathsf{ran},(\tau,\iota),t}, \theta_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\eta}_{\mathsf{ran},(\tau,\iota),t},\ \vec{\eta}_{\mathsf{del},(\tau,\iota),t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t},$$
$$(t=0,...,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},$$

$$s_{\mathsf{ran},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathsf{ran},(\tau,\iota),t},\ s_{\mathsf{del},(\tau,\iota),0} := \sum_{t=1}^{L+1} s_{\mathsf{del},(\tau,\iota),t},$$

[数140]

$$
\begin{aligned}
k^*_{L,\mathsf{dec}} &:= (\ (-s_{\mathsf{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}^*_0}, \\
&\quad (s_{\mathsf{dec},t}\ \vec{e}_{t,1} + \theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L), \\
k^*_{L,\mathsf{ran},j} &:= (\ (-s_{\mathsf{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0}, \\
&\quad (s_{\mathsf{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t} \\
&\quad : t = 1,\ldots,L), \\
k^*_{L,\mathsf{ran},(\tau,\iota)} &:= (\ (-s_{\mathsf{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0}, \\
&\quad (s_{\mathsf{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t} \\
&\quad : t = 1,\ldots,L \\
&\quad (s_{\mathsf{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1},\ 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}), \\
k^*_{L,\mathsf{del},(\tau,\iota)} &:= (\ (-s_{\mathsf{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0}, \\
&\quad (s_{\mathsf{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t} \\
&\quad : t = 1,\ldots,L \\
&\quad (s_{\mathsf{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}), \\
\mathsf{sk}_L &:= (k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L}, \\
&\quad \{k^*_{L,\mathsf{ran},(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}, \\
&\quad \{k^*_{L,\mathsf{del},(\tau,\iota)}\}_{\tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}), \\
&\text{return } \mathsf{sk}_L.
\end{aligned}
$$

[0054] 暗号化装置２００の機能と動作とについて説明する。

図９に示すように、暗号化装置２００は、マスター公開鍵取得部２１０、情報入力部２２０（第２情報入力部）、暗号化データ生成部２３０、データ送信部２４０を備える。

また、情報入力部２２０は、属性情報入力部２２１、メッセージ入力部２２２を備える。また、暗号化データ生成部２３０は、乱数生成部２３１、暗号化データｃ１生成部２３２、暗号化データｃ２生成部２３３を備える。

[0055] 図１４に基づき、暗号化装置２００が実行するＥｎｃアルゴリズムの処理

について説明する。

（Ｓ３０１：マスター公開鍵取得ステップ）

マスター公開鍵取得部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が生成したマスター公開鍵ｐｋを取得する。

[0056] （Ｓ３０２：情報入力ステップ）

属性情報入力部２２１は、入力装置により、属性情報（$\vec{x}_1$，．．．，$\vec{x}_L$）：＝（（$x_{1,i}$（ｉ＝１，．．．，n_1））），．．．，（$x_{L,i}$（ｉ＝１，．．．，n_L））））を入力する。なお、属性情報としては、暗号化したメッセージを復号可能な者の属性が入力される。

また、メッセージ入力部２２２は、入力装置により、暗号化するメッセージｍを入力する。

[0057] （Ｓ３０３：乱数生成ステップ）

乱数生成部２３１は、処理装置により、乱数（$\vec{x}_{L+1}$，．．．，$\vec{x}_d$）：＝（（$x_{L+1,i}$（ｉ＝１，．．．，n_{L+1}））），．．．，（$x_{d,i}$（ｉ＝１，．．．，n_d））））と、乱数ω，ζ，$\vec{\phi}_t$（ｔ＝０，．．．，ｄ）とを数１４１に示すように生成する。

[数141]

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) := ((x_{L+1,1},\ldots,x_{L+1,n_{L+1}}),\ldots,(x_{d,1},\ldots,x_{d,n_d}))$$
$$\xleftarrow{U} \mathbb{F}_q^{n_{L+1}} \times \cdots \times \mathbb{F}_q^{n_d},$$
$$\omega,\zeta \xleftarrow{U} \mathbb{F}_q,$$
$$\vec{\varphi}_t := (\varphi_{t,1},\ldots,\varphi_{t,z_t}) \xleftarrow{U} \mathbb{F}_q^{z_t} \quad (t=0,\ldots,d)$$

[0058] （Ｓ３０４：暗号化データｃ１生成ステップ）

暗号化データｃ１生成部２３２は、処理装置により、暗号化データｃｔの要素である暗号化データc_1を数１４２に示すように生成する。

[数142]

$$c_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1, ..., d)$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１４２は、以下のように、基底$Ｂ_0$及び基底$Ｂ_t$（ｔ＝１，．．．，ｄ）の基底ベクトルの係数が設定され、暗号化データ$ｃ_1$が生成されることを意味する。

まず、基底$Ｂ_0$の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$ｂ_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$ｂ_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$ｂ_{0,1}$，．．．，$ｂ_{0,3}$を意味する。

基底$Ｂ_0$の基底ベクトル１の係数としてωが設定される。基底ベクトル１＋１，．．．，１＋$ｕ_0$の係数として０が設定される。基底ベクトル１＋$ｕ_0$＋１の係数としてζが設定される。基底ベクトル１＋$ｕ_0$＋１＋１，．．．，１＋$ｕ_0$＋１＋$ｗ_0$の係数として０が設定される。基底ベクトル１＋$ｕ_0$＋１＋$ｗ_0$＋１，．．．，１＋$ｕ_0$＋１＋$ｗ_0$＋$ｚ_0$の係数として$φ_{0,1}$，．．．，$φ_{0,z}$。（ここで、ｚ０は$ｚ_0$のことである）が設定される。

次に、基底$Ｂ_t$（ｔ＝１，．．．，ｄ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$ｂ_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$ｂ_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$ｂ_{t,1}$，．．．，$ｂ_{t,3}$を意味する。

基底$Ｂ_t$（ｔ＝１，．．．，ｄ）の基底ベクトル１，．．．，$ｎ_t$の係数として$ωｘ_{t,1}$，．．．，$ωｘ_{t,nt}$（ここで、ｎｔは$ｎ_t$のことである）が設定される。基底ベクトル$ｎ_t$＋１，．．．，$ｎ_t$＋$ｕ_t$＋$ｗ_t$の係数として０が設定される。基底ベクトル$ｎ_t$＋$ｕ_t$＋$ｗ_t$＋１，．．．，$ｎ_t$＋$ｕ_t$＋$ｗ_t$＋$ｚ_t$の係数として$φ_{t,1}$，．．．，$φ_{t,zt}$（ここで、ｚｔは$ｚ_t$のことである）が

設定される。

[0059] （Ｓ３０５：暗号化データｃ２生成ステップ）

暗号化データｃ２生成部２３３は、処理装置により、暗号化データｃｔの要素である暗号化データc_2を数１４３に示すように生成する。

[数143]

$$c_2 := g_T^{\zeta} m$$

[0060] （Ｓ３０６：データ送信ステップ）

データ送信部２４０は、暗号化データc_1と、暗号化データc_2とを含む暗号化データｃｔ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、暗号化データｃｔは、他の方法により復号装置３００へ送信されてもよい。

[0061] つまり、（Ｓ３０１）から（Ｓ３０５）において、暗号化装置２００は数１４４に示すＥｎｃアルゴリズムを実行して、暗号化データｃｔを生成する。そして、（Ｓ３０６）で、暗号化装置２００は生成された暗号化データｃｔを復号装置３００へ送信する。

[数144]

$$\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):\\
&(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\cup} \mathbb{F}_q^{n_{L+1}} \times \cdots \times \mathbb{F}_q^{n_d};\\
&\omega,\zeta \xleftarrow{\cup} \mathbb{F}_q,\ \vec{\varphi}_t \xleftarrow{\cup} \mathbb{F}_q^{z_t}\ (t=0,\ldots,d),\\
&c_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t=1,\ldots,d),\\
&c_2 := g_T^{\zeta} m,\\
&\mathsf{ct} := (c_1, c_2),\\
&\text{return } \mathsf{ct}.
\end{aligned}$$

[0062] 復号装置３００の機能と動作とについて説明する。

図１０に示すように、復号装置３００は、復号鍵取得部３１０、データ受信部３２０、ペアリング演算部３３０、メッセージ計算部３４０を備える。

[0063] 図１５に基づき、復号装置３００が実行する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３１０は、例えば、通信装置によりネットワークを介して、復号鍵sk_Lを取得する。また、復号鍵取得部３１０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。

[0064] （Ｓ４０２：データ受信ステップ）

データ受信部３２０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が送信した暗号化データｃｔを受信する。

[0065] （Ｓ４０３：ペアリング演算ステップ）

ペアリング演算部３３０は、処理装置により、数１４５に示すペアリング演算を行い、セッション鍵Ｋ＝g_T^{ζ}を計算する。

[数145]

$$K := e(c_1, k^*_{L,\mathsf{dec}})$$

なお、（$v^{\rightarrow}_1$，．．．，$v^{\rightarrow}_L$）と（$x^{\rightarrow}_1$，．．．，$x^{\rightarrow}_L$）との内積が０であれば、数１４５を計算することにより、セッション鍵Ｋが計算される。

[0066] （Ｓ４０４：メッセージ計算ステップ）

メッセージ計算部３４０は、処理装置により、暗号化データｃ２をセッション鍵Ｋで割ることにより、メッセージｍ’（＝ｍ）を計算する。

[0067] つまり、（Ｓ４０１）から（Ｓ４０４）において、復号装置３００は数１４６に示すＤｅｃアルゴリズムを実行して、メッセージｍ’（＝ｍ）を計算する。

[数146]

$$\mathsf{Dec}(\mathsf{pk}, k^*_{L,\mathsf{dec}}, \mathsf{ct}):\ m' := c_2 / e(c_1, k^*_{L,\mathsf{dec}})$$
$$\text{return } m'.$$

[0068] 鍵委譲装置４００の機能と動作とについて説明する。

図１１に示すように、鍵委譲装置４００は、復号鍵取得部４１０、情報入力部４２０（第３情報入力部）、委譲鍵生成部４３０、鍵配布部４４０（委譲鍵送信部）を備える。

また、委譲鍵生成部４３０は、乱数生成部４３１、下位復号要素生成部４３２、下位ランダム化要素生成部４３３、下位委譲要素生成部４３４を備える。

[0069] 図１６に基づき、鍵委譲装置４００が実行するＤｅｌｅｇａｔｅ$_{L}$アルゴリズムの処理について説明する。

（Ｓ５０１：復号鍵取得ステップ）

復号鍵取得部４１０は、例えば、通信装置によりネットワークを介して、復号鍵ｓｋ$_{L}$を取得する。また、復号鍵取得部４１０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。

[0070] （Ｓ５０２：情報入力ステップ）

情報入力部４２０は、入力装置により、述語情報$\vec{v}_{L+1}$：＝（$v_{L+1,i}$（ｉ＝１，．．．，n_{L+1}））を入力する。なお、述語情報としては、鍵を委譲される者の属性が入力される。

[0071] （Ｓ５０３：乱数生成ステップ）

乱数生成部４３１は、処理装置により、ｊ＝１，．．．，２Ｌと，ｊ’＝１，．．．，２（Ｌ＋１）と，τ＝Ｌ＋２，．．．，ｄと，（τ，ι）＝（τ，１），．．．，（τ，n_{τ}）と，ｔ＝０，．．．，Ｌ＋１，τと，（ｔ，ｉ）＝（ｔ，１），．．．，（ｔ，n_{t}）との各整数ｊ，ｊ’，τ，ι，ｔ，ｉについて、乱数$\alpha_{dec,j}$，σ_{dec}，$\alpha_{ran,j',j}$，$\sigma_{ran,j'}$，$\alpha_{ran,(\tau,\iota),j}$，$\sigma_{ran,(\tau,\iota)}$，$\phi_{ran,(\tau,\iota)}$，$\alpha_{del,(\tau,\iota),j}$，$\sigma_{del,(\tau,\iota)}$，$\phi_{del,(\tau,\iota)}$，$\phi'$，$\eta_{dec,(t,i)}$，$\eta_{ran,j',(t,i)}$，$\eta_{ran,(\tau,\iota),(t,i)}$，$\eta_{del,(\tau,\iota),(t,i)}$を数１４７に示すように生成する。

[数147]

$$\text{for } j=1,...,2L;\ j'=1,...,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$$
$$t=0,...,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$$
$$\alpha_{\mathrm{dec},j},\ \sigma_{\mathrm{dec}},\ \alpha_{\mathrm{ran},j',j},\ \sigma_{\mathrm{ran},j'},\ \alpha_{\mathrm{ran},(\tau,\iota),j},\sigma_{\mathrm{ran},(\tau,\iota)},$$
$$\phi_{\mathrm{ran},(\tau,\iota)},\ \alpha_{\mathrm{del},(\tau,\iota),j},\ \sigma_{\mathrm{del},(\tau,\iota)},\ \phi_{\mathrm{del},(\tau,\iota)},\ \psi',$$
$$\eta_{\mathrm{dec},(t,i)},\ \eta_{\mathrm{ran},j',(t,i)},\ \eta_{\mathrm{ran},(\tau,\iota),(t,i)},\ \eta_{\mathrm{del},(\tau,\iota),(t,i)} \xleftarrow{\cup} \mathbb{F}_q$$

[0072] （Ｓ５０４：下位復号要素生成ステップ）

下位復号要素生成部４３２は、処理装置により、委譲鍵ｓｋ$_{L+1}$の要素である下位復号要素ｋ*$_{L+1,\,dec}$を数１４８に示すように生成する。

[数148]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L}\alpha_{\mathrm{dec},j}k^*_{L,\mathrm{ran},j}$$
$$+\sigma_{\mathrm{dec}}\Big(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathrm{del},(L+1,i)}\Big)+\sum_{i=1}^{w_t}\eta_{\mathrm{dec},(0,i)}b^*_{0,1+u_0+1+i}$$
$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathrm{dec},(t,i)}b^*_{t,n_t+u_t+i}$$

[0073] （Ｓ５０５：第１下位ランダム化要素生成ステップ）

下位ランダム化要素生成部４３３は、処理装置により、ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’について、委譲鍵ｓｋ$_{L+1}$の要素である第１下位ランダム化要素ｋ*$_{L+1,\,ran,\,j'}$を数１４９に示すように生成する。

[数149]

$$k^*_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L}\alpha_{\mathrm{ran},j',j}k^*_{L,\mathrm{ran},j}$$
$$+\sigma_{\mathrm{ran},j'}\Big(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathrm{del},(L+1,i)}\Big)$$
$$+\sum_{i=1}^{w_t}\eta_{\mathrm{ran},j',(0,i)}b^*_{0,1+u_0+1+i}$$
$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathrm{ran},j',(t,i)}b^*_{t,n_t+u_t+i}$$

[0074] （Ｓ５０６：第２下位ランダム化要素生成ステップ）

下位ランダム化要素生成部４３３は、処理装置により、τ＝Ｌ＋２，．．．，ｄの各整数τと、各整数τに関してι＝１，．．．．，n_τの各整数ιについて、委譲鍵sk_{L+1}の要素である第２下位ランダム化要素$k^*_{L+1,ran,(\tau,\iota)}$を数１５０に示すように生成する。

[数150]

$$k^*_{L+1,\mathrm{ran},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota),j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{ran},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \phi_{\mathrm{ran},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

[0075] （Ｓ５０７：下位委譲要素生成ステップ）

下位委譲要素生成部４３４は、処理装置により、τ＝Ｌ＋２，．．．，ｄの各整数τと、各整数τについてι＝１，．．．，n_τの各整数ιについて、委譲鍵sk_{L+1}の要素である下位委譲要素$k^*_{L+1,del,(\tau,\iota)}$を数１５１に示すように生成する。

[数151]

$$k^*_{L+1,\mathrm{del},(\tau,\iota)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota),j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{del},(\tau,\iota)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \right) + \psi' k^*_{L,\mathrm{del},(\tau,\iota)} + \phi_{\mathrm{del},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$

[0076] （Ｓ５０８：鍵配布ステップ）

鍵配布部１５０は、下位復号要素$k^*_{L+1,dec}$と、第１下位ランダム化要素$k^*_{L+1,ran,j'}$（j'＝1，．．．，２（Ｌ＋１））と、第２下位ランダム化要素$k^*_{L+1,ran,(\tau,\iota)}$（$\tau$＝Ｌ＋２，．．．，ｄ；（$\tau$，$\iota$）＝（$\tau$，１），．．．，（$\tau$，$n_\tau$））と、下位委譲要素$k^*_{L+1,del,(\tau,\iota)}$（$\tau$＝Ｌ＋２，．．．，ｄ；（$\tau$，$\iota$）＝（$\tau$，１），．．．，（$\tau$，$n_\tau$））とを要素とする委譲鍵$sk_{L+1}$（下位の復号鍵）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下位の復号装置３００へ配布する。もちろん、委譲鍵sk_{L+1}は、他の方法により下位の復号装置３００へ配布されてもよい。

[0077] つまり、（Ｓ５０１）から（Ｓ５０７）において、鍵委譲装置４００は数１５２、１５３に示す$Delegate_L$アルゴリズムを実行して、委譲鍵sk_{L+1}を生成する。そして、（Ｓ５０８）で、鍵委譲装置４００は生成された委譲鍵sk_{L+1}を下位の復号装置３００へ配布する。

[数152]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,\vec{v}_{L+1}:=(v_{L+1,1},\ldots,v_{L+1,n_{L+1}})):$$

$$\text{for } j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$

$$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$$

$$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\ \sigma_{\mathsf{ran},(\tau,\iota)},$$

$$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$$

$$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

[数153]

$$
\begin{aligned}
k^*_{L+1,\mathrm{dec}} &:= k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L} \alpha_{\mathrm{dec},j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{dec}} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \Big) + \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(t,i)} b^*_{t,n_t+u_t+i}, \\
k^*_{L+1,\mathrm{ran},j'} &:= \sum_{j=1}^{2L} \alpha_{\mathrm{ran},j',j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{ran},j'} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \Big) + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^*_{t,n_t+u_t+i}, \\
k^*_{L+1,\mathrm{ran},(\tau,\iota)} &:= \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota),j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{ran},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \Big) \\
&\quad + \phi_{\mathrm{ran},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} \\
&\quad + \sum_{i=1}^{w_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}, \\
k^*_{L+1,\mathrm{del},(\tau,\iota)} &:= \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota),j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{del},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)} \Big) + \psi' k^*_{L,\mathrm{del},(\tau,\iota)} \\
&\quad + \phi_{\mathrm{del},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} \\
&\quad + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}, \\
\mathsf{sk}_{L+1} &:= \big(k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)}, \\
&\qquad \{k^*_{L+1,\mathrm{ran},(\tau,\iota)}, k^*_{L+1,\mathrm{del},(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)} \big), \\
&\text{return } \mathsf{sk}_{L+1}
\end{aligned}
$$

[0078] なお、下位の復号装置３００が、委譲鍵ｓｋ$_{L+1}$を用いてＤｅｃアルゴリズムを実行した場合、図１５の（Ｓ４０３）では、（$\vec{v}_1$，．．．，$\vec{v}_{L+1}$）と（$\vec{x}_1$，．．．，$\vec{x}_{L+1}$）との内積が０であれば、数１４５を計算するこ

とにより、セッション鍵Ｋが計算される。

[0079] 以上のように、実施の形態１に係る暗号処理システム１０は、ｄ＋１個のＮ$_t$（ｔ＝０，．．．，ｄ）次元空間を用いて、ｄ階層の階層的内積述語暗号方式を実現する。ここで、第Ｌ層目（１≦Ｌ≦ｄ）の暗号処理に必要な空間は、Ｌ＋１個のＮ$_t$（ｔ＝０，．．．，Ｌ）次元空間である。したがって、鍵のサイズを小さくでき、演算等の効率をよくすることができる。また、鍵を記録するメモリやレジスタ等の領域も小さくなる。

[0080] なお、上記説明において、ｕ$_t$、ｗ$_t$、ｚ$_t$（ｔ＝０，．．．，ｄ）の次元は、安全性を高めるために設けた次元である。したがって、安全性が低くなってしまうが、ｕ$_t$、ｗ$_t$、ｚ$_t$（ｔ＝０，．．．，ｄ）をそれぞれ０として、ｕ$_t$、ｗ$_t$、ｚ$_t$（ｔ＝０，．．．，ｄ）の次元を設けなくてもよい。

[0081] また、上記説明では、Ｎ$_0$に１＋ｕ$_0$＋１＋ｗ$_0$＋ｚ$_0$を設定し、Ｎ$_t$にｎ$_t$＋ｕ$_t$＋ｗ$_t$＋ｚ$_t$を設定した。しかし、１＋ｕ$_0$＋１＋ｗ$_0$＋ｚ$_0$を１＋１＋１＋１＋１としてＮ$_0$に５を設定し、ｎ$_t$＋ｕ$_t$＋ｗ$_t$＋ｚ$_t$をｎ$_t$＋ｎ$_t$＋ｎ$_t$＋１としてＮ$_t$に３ｎ$_t$＋１を設定してもよい。

この場合、数１３２に示すＳｅｔｕｐアルゴリズムは、数１５４のように書き換えられる。なお、Ｇ$_{ob}$は数１５５のように書き換えられる。

[数154]

$$\mathsf{Setup}(1^\lambda, \vec{n} := (d; n_1, ..., n_d): \ (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,...,d}) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}(1^\lambda, \vec{n}),$$

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,3}, b_{0,5}),\ \hat{\mathbb{B}}_t := (b_{t,1}, .., b_{t,n_t}, b_{t,3n_t+1}) \quad \text{for } t = 1, .., d,$$

$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,3}^*),\ \hat{\mathbb{B}}_t^* := (b_{t,1}^*, .., b_{t,n_t}^*) \text{for } t = 1, .., d,$$

$$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\vec{n}}, \{\hat{\mathbb{B}}_t\}_{t=0,...,d}, b_{0,4}^*, \{b_{t,2n_t+1}^*, ..., b_{t,3n_t}^*\}_{t=1,...,d}),$$

$$\mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,...,d},$$

return pk, sk.

[数155]

$$\mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}:=(d;n_1,...,n_d)):$$
$$N_0:=5,\ N_t:=3n_t+1\ (t=1,...,d),$$
$$\mathsf{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{\mathsf{R}}\mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),$$
$$\psi\xleftarrow{\mathsf{U}}\mathbb{F}_q^{\times},$$
$$\text{For } t=0,\ldots,d,$$
$$\mathsf{param}_{\mathbb{V}_t}:=(q,\mathbb{V}_t,\mathbb{G}_T,\mathbb{A}_t,e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t,\mathsf{param}_{\mathbb{G}}),$$
$$X_t:=(\chi_{t,i,j})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t,\mathbb{F}_q),\quad (\nu_{t,i,j})_{i,j}:=\psi\cdot(X_t^{\mathrm{T}})^{-1},$$
$$b_{t,i}:=(\chi_{t,i,1},\ldots,\chi_{t,i,N_t})_{\mathbb{A}_t}=\sum_{j=1}^{N_t}\chi_{t,i,j}a_{t,j},\ \mathbb{B}_t:=(b_{t,1},\ldots,b_{t,N_t}),$$
$$b_{t,i}^{*}:=(\nu_{t,i,1},\ldots,\nu_{t,i,N_t})_{\mathbb{A}_t}=\sum_{j=1}^{N_t}\nu_{t,i,j}a_{t,j},\ \mathbb{B}_t^{*}:=(b_{t,1}^{*},\ldots,b_{t,N_t}^{*}),$$
$$g_T:=e(g,g)^{\psi},\quad \mathsf{param}_n^{*}:=(\{\mathsf{param}_{\mathbb{V}_t}\}_{t=1,\ldots,d},g_T)$$
$$\text{return } (\mathsf{param}_n^{*},\{\mathbb{B}_t,\mathbb{B}_t^{*}\}_{t=0,\ldots,d}).$$

また、数１３９、数１４０に示すＫｅｙＧｅｎアルゴリズムは、数１５６、数１５７のように書き換えられる。

[数156]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\ldots,\vec{v}_L):=(v_{1,1},\ldots,v_{1,n_1}),\ldots,\ (v_{L,1},\ldots,v_{L,n_L})):$$
$$\text{for } j=1,\ldots,2L;\ \tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$
$$\psi,s_{\mathsf{dec},t},s_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q\ (t=1,\ldots,L);$$
$$\theta_{\mathsf{dec},t},\theta_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\ \vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t}\ (t=0,\ldots,L);$$
$$s_{\mathsf{ran},(\tau,\iota),t},s_{\mathsf{del},(\tau,\iota),t}\xleftarrow{\mathsf{U}}\mathbb{F}_q\ (t=1,\ldots,L+1);$$
$$\theta_{\mathsf{ran},(\tau,\iota),t},\theta_{\mathsf{del},(\tau,\iota),t}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\ \vec{\eta}_{\mathsf{ran},(\tau,\iota),t},\ \vec{\eta}_{\mathsf{del},(\tau,\iota),t}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t},$$
$$(t=0,\ldots,L+1);$$
$$s_{\mathsf{dec},0}:=\sum_{t=1}^{L}s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},j,t},$$
$$s_{\mathsf{ran},(\tau,\iota),0}:=\sum_{t=1}^{L+1}s_{\mathsf{ran},(\tau,\iota),t},\ s_{\mathsf{del},(\tau,\iota),0}:=\sum_{t=1}^{L+1}s_{\mathsf{del},(\tau,\iota),t},$$

[数157]

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0},0,1,\eta_{\mathsf{dec},0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{dec},t}\ \vec{e}_{t,1}+\theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{dec},t},0)_{\mathbb{B}^*_t} : t=1,...,L),$$
$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0},0,0,\eta_{\mathsf{ran},j,0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},j,t}\ \vec{e}_{t,1}+\theta_{\mathsf{ran},j,t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{ran},j,t},0)_{\mathbb{B}^*_t}$$
$$: t=1,...,L),$$
$$k^*_{L,\mathsf{ran},(\tau,\iota)} := (\ (-s_{\mathsf{ran},(\tau,\iota),0},0,0,\eta_{\mathsf{ran},(\tau,\iota),0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},(\tau,\iota),t}\ \vec{e}_{t,1}+\theta_{\mathsf{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{ran},(\tau,\iota),t},0)_{\mathbb{B}^*_t}$$
$$: t=1,...,L$$
$$(s_{\mathsf{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1},\ 0^{n_\tau},\vec{\eta}_{\mathsf{ran},(\tau,\iota),L+1},0)_{\mathbb{B}^*_\tau}),$$
$$k^*_{L,\mathsf{del},(\tau,\iota)} := (\ (-s_{\mathsf{del},(\tau,\iota),0},0,0,\eta_{\mathsf{del},(\tau,\iota),0},0)_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{del},(\tau,\iota),t}\ \vec{e}_{t,1}+\theta_{\mathsf{del},(\tau,\iota),t}\vec{v}_t,\ 0^{n_t},\vec{\eta}_{\mathsf{del},(\tau,\iota),t},0)_{\mathbb{B}^*_t}$$
$$: t=1,...,L$$
$$(s_{\mathsf{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1}+\psi\vec{e}_{\tau,\iota},0^{n_\tau},\vec{\eta}_{\mathsf{del},(\tau,\iota),L+1},0)_{\mathbb{B}^*_\tau}),$$
$$\mathsf{sk}_L := (k^*_{L,\mathsf{dec}},\{k^*_{L,\mathsf{ran},j}\}_{j=1,...,2L},$$
$$\{k^*_{L,\mathsf{ran},(\tau,\iota)}\}_{\tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau)},$$
$$\{k^*_{L,\mathsf{del},(\tau,\iota)}\}_{\tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau)}),$$
return sk_L.

また、数１４４に示すＥｎｃアルゴリズムは、数１５８のように書き換えられる。

[数158]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_{L+1}} \times \cdots \times \mathbb{F}_q^{n_d};\ \omega,\zeta,\varphi_0,\ldots,\varphi_d \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$c_1 := ((\omega,0,\zeta,0,\varphi_0)_{\mathbb{B}_0}, (\omega\vec{x}_t,0^{n_t},0^{n_t},\varphi_t)_{\mathbb{B}t} : t=1,\ldots,d),$$

$$c_2 := g_T^{\zeta} m,$$

$$\mathsf{ct} := (c_1,c_2),$$

return ct.

また、数１５２、数１５３に示すＤｅｌｅｇａｔｅ$_L$アルゴリズムは、数１５９、数１６０のように書き換えられる。

[数159]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,\vec{v}_{L+1} := (v_{L+1,1},\ldots,v_{L+1,n_{L+1}})):$$

$$\text{for } j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$

$$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,n_t);$$

$$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\ \sigma_{\mathsf{ran},(\tau,\iota)},$$

$$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$$

$$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

[数160]

$$
\begin{aligned}
k^*_{L+1,\mathsf{dec}} &:= k^*_{L,\mathsf{dec}} + \sum_{j=1}^{2L} \alpha_{\mathsf{dec},j}\, k^*_{L,\mathsf{ran},j} \\
&\quad + \sigma_{\mathsf{dec}} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)} \Big) + \eta_{\mathsf{dec},(0,1)} b^*_{0,4} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{dec},(t,i)} b^*_{t,2n_t+i}, \\
k^*_{L+1,\mathsf{ran},j'} &:= \sum_{j=1}^{2L} \alpha_{\mathsf{ran},j',j}\, k^*_{L,\mathsf{ran},j} \\
&\quad + \sigma_{\mathsf{ran},j'} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)} \Big) + \eta_{\mathsf{ran},j',(0,1)} b^*_{0,4} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{ran},j',(t,i)} b^*_{t,2n_t+i}, \\
k^*_{L+1,\mathsf{ran},(\tau,\iota)} &:= \sum_{j=1}^{2L} \alpha_{\mathsf{ran},(\tau,\iota),j}\, k^*_{L,\mathsf{ran},j} \\
&\quad + \sigma_{\mathsf{ran},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)} \Big) \\
&\quad + \phi_{\mathsf{ran},(\tau,\iota)} k^*_{L,\mathsf{ran},(\tau,\iota)} + \eta_{\mathsf{ran},(\tau,\iota),(0,1)} b^*_{0,4} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{ran},(\tau,\iota),(t,i)} b^*_{t,2n_t+i} \\
&\quad + \sum_{i=1}^{n_\tau} \eta_{\mathsf{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,2n_\tau+i}, \\
k^*_{L+1,\mathsf{del},(\tau,\iota)} &:= \sum_{j=1}^{2L} \alpha_{\mathsf{del},(\tau,\iota),j}\, k^*_{L,\mathsf{ran},j} \\
&\quad + \sigma_{\mathsf{del},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathsf{del},(L+1,i)} \Big) + \psi' k^*_{L,\mathsf{del},(\tau,\iota)} \\
&\quad + \phi_{\mathsf{del},(\tau,\iota)} k^*_{L,\mathsf{ran},(\tau,\iota)} + \eta_{\mathsf{del},(\tau,\iota),(0,1)} b^*_{0,4} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathsf{del},(\tau,\iota),(t,i)} b^*_{t,2n_t+i} \\
&\quad + \sum_{i=1}^{n_\tau} \eta_{\mathsf{del},(\tau,\iota),(\tau,i)} b^*_{\tau,2n_\tau+i}, \\
\mathsf{sk}_{L+1} &:= \big(k^*_{L+1,\mathsf{dec}}, \{k^*_{L+1,\mathsf{ran},j'}\}_{j'=1,\ldots,2(L+1)}, \\
&\qquad \{k^*_{L+1,\mathsf{ran},(\tau,\iota)}, k^*_{L+1,\mathsf{del},(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)} \big), \\
\text{return } & \mathsf{sk}_{L+1}
\end{aligned}
$$

なお、数１４６に示すＤｅｃアルゴリズムに変更はない。

[0082] また、Ｓｅｔｕｐアルゴリズムは、暗号処理システム１０のセットアップ時に一度実行すればよく、復号鍵を生成する度に実行する必要はない。また

、上記説明では、ＳｅｔｕｐアルゴリズムとＫｅｙＧｅｎアルゴリズムとを鍵生成装置１００が実行するとしたが、ＳｅｔｕｐアルゴリズムとＫｅｙＧｅｎアルゴリズムとをそれぞれ異なる装置が実行するとしてもよい。

[0083] 実施の形態２．

この実施の形態では、実施の形態１で説明した方式を一般化した階層的内積述語暗号方式について説明する。

[0084] 実施の形態１で説明した階層的内積述語暗号方式では、原則として暗号化データｃｔに設定された属性情報と、復号鍵に設定された述語情報との内積が０の場合に、暗号化データｃｔを復号鍵で復号可能であった。

しかし、実施の形態２で説明する階層的内積述語暗号方式では、暗号化データｃｔに設定された属性情報と、復号鍵に設定された述語情報との内積が０とならない場合であっても復号可能となるように設定できる。

具体的には、以下の説明において、ρ_t（ｔ＝１，．．．，ｄ）の値が０である整数ｔについては、属性情報$\vec{x}_t$と述語情報$\vec{v}_t$との内積が０となり、ρ_t（ｔ＝１，．．．，ｄ）の値が１である整数ｔについては、属性情報$\vec{x}_t$と述語情報$\vec{v}_t$との内積が０とならない場合に、復号可能となる。

これにより、例えば、ρ_t（ｔ＝１，．．．，ｄ）の値の設定に応じて、肯定形の条件式（例えば、属性情報＝述語情報）と否定形の条件式（属性情報≠述語情報）との設定をすることができる。

[0085] 図１７から図１９に基づき、実施の形態２に係る階層的内積述語暗号方式、及び、階層的内積述語暗号方式を実行する暗号処理システム１０の機能と動作とについて説明する。

なお、実施の形態２に係る暗号処理システム１０の機能構成については、図８から図１１に示す実施の形態１に係る暗号処理システム１０の機能構成と同一である。

図１７は、鍵生成装置１００の動作を示すフローチャートであり、ＫｅｙＧｅｎアルゴリズムの処理を示すフローチャートである。図１８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。図１９は、鍵委譲装置４００の動作を示すフローチャートであり、$Delegate_L$アルゴリズムの処理を示すフローチャートである。

なお、実施の形態２に係るＳｅｔｕｐアルゴリズムとＥｎｃアルゴリズムとの処理は、実施の形態１に係るＳｅｔｕｐアルゴリズムとＥｎｃアルゴリズムとの処理と同一であるため、説明を省略する。但し、Ｅｎｃアルゴリズムでは、暗号化データｃｔに、暗号化データc_1，c_2だけでなく、属性情報$\vec{x}_i$（ｉ＝１，．．．，Ｌ）も含めて、復号装置３００へ送信する。

[0086] 図１７に基づき、鍵生成装置１００が実行するＫｅｙＧｅｎアルゴリズムの処理について説明する。

（Ｓ６０１：情報入力ステップ）

情報入力部１３０は、入力装置により、述語情報$((\vec{v}_1, \rho_1), \ldots, (\vec{v}_L, \rho_L)) := ((v_{1,i}\ (i=1,\ldots,n_1), \rho_1 \in \{0,1\}), \ldots, (v_{L,i}\ (i=1,\ldots,n_L), \rho_L \in \{0,1\}))$を入力する。なお、述語情報としては、鍵を使用する者の属性が入力される。

[0087] （Ｓ６０２：乱数生成ステップ）

乱数生成部１４１は、処理装置により、$j=1,\ldots,2L$と、$\tau=L+1,\ldots,d$と、$(\tau, \iota)=(\tau,1),\ldots,(\tau,n_\tau)$との各整数$j$，$\tau$，$\iota$について、乱数$\phi$と、乱数$s_{dec,t}$，$s_{ran,j,t}$（$t=1,\ldots,L$）と、乱数$\theta_{dec,t}$，$\theta_{ran,j,t}$，$\vec{\eta}_{dec,t}$，$\vec{\eta}_{ran,j,t}$，$\vec{\eta}_{ran,0,t}$，$\vec{\eta}_{del,0,t}$，$\vec{\eta}_{del,1,t}$（$t=0,\ldots,L$）と、乱数$s_{ran,0,t}$，$s_{del,0,t}$，$s_{del,1,t}$（$t=0,\ldots,L+1$）と、乱数$\theta_{ran,0,t}$，$\theta_{del,0,t}$，$\theta_{del,1,t}$（$t=0,\ldots,L+1$）と、乱数$\vec{\eta}_{ran,(\tau,\iota)}$，$\vec{\eta}_{del,0,(\tau,\iota)}$，$\vec{\eta}_{del,1,(\tau,\iota)}$とを数１６１に示すように生成する。

[数161]

$$\text{for } j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$$

$$\psi, s_{\mathrm{dec},t}, s_{\mathrm{ran},j,t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=1,...,L),$$

$$\theta_{\mathrm{dec},t}, \theta_{\mathrm{ran},j,t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{dec},t} := (\eta_{\mathrm{dec},t,1},...,\eta_{\mathrm{dec},t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{ran},j,t} := (\eta_{\mathrm{ran},j,t,1},...,\eta_{\mathrm{ran},j,t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{ran},0,t} := (\eta_{\mathrm{ran},0,t,1},...,\eta_{\mathrm{ran},0,t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{del},0,t} := (\eta_{\mathrm{del},0,t,1},...,\eta_{\mathrm{del},0,t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$\vec{\eta}_{\mathrm{del},1,t} := (\eta_{\mathrm{del},1,t,1},...,\eta_{\mathrm{del},1,t,w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t} \ (t=0,...,L),$$

$$s_{\mathrm{ran},0,t}, s_{\mathrm{del},0,t}, s_{\mathrm{del},1,t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=1,...,L+1),$$

$$\theta_{\mathrm{ran},0,t}, \theta_{\mathrm{del},0,t}, \theta_{\mathrm{del},1,t} \xleftarrow{\mathrm{U}} \mathbb{F}_q \ (t=0,...,L+1),$$

$$\vec{\eta}_{\mathrm{ran},0,(\tau,\iota)} := (\eta_{\mathrm{ran},0,(\tau,\iota),1},...,\eta_{\mathrm{ran},0,(\tau,\iota),w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t},$$

$$\vec{\eta}_{\mathrm{del},0,(\tau,\iota)} := (\eta_{\mathrm{del},0,(\tau,\iota),1},...,\eta_{\mathrm{del},0,(\tau,\iota),w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t},$$

$$\vec{\eta}_{\mathrm{del},1,(\tau,\iota)} := (\eta_{\mathrm{del},1,(\tau,\iota),1},...,\eta_{\mathrm{del},1,(\tau,\iota),w_t}) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{w_t}$$

また、数１６２に示すように$s_{dec,0}$と、$s_{ran,j,0}$と、$s_{ran,0,0}$と、$s_{del,0,0}$と、$s_{del,1,0}$とを設定する。

[数162]

$$s_{\mathrm{dec},0} := \sum_{t=1}^{L} s_{\mathrm{dec},t},$$

$$s_{\mathrm{ran},j,0} := \sum_{t=1}^{L} s_{\mathrm{ran},j,t},$$

$$s_{\mathrm{ran},0,0} := \sum_{t=1}^{L} s_{\mathrm{ran},0,t},$$

$$s_{\mathrm{del},0,0} := \sum_{t=1}^{L+1} s_{\mathrm{del},0,t},$$

$$s_{\mathrm{del},1,0} := \sum_{t=1}^{L+1} s_{\mathrm{del},1,t}$$

[0088] （Ｓ６０３：復号要素生成ステップ）

復号要素生成部１４２は、処理装置により、復号鍵ｓｋ$_L$の要素である復号要素ｋ*$_{L,dec}$を数１６３に示すように生成する。

[数163]

$$k^*_{L,\mathrm{dec}} := \Big((-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},\ \left\{ \begin{array}{ll} (s_{\mathrm{dec},t}\vec{e}_{t,1} + \theta_{\mathrm{dec},t}, \vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \mathrm{if}\ \rho_t = 0 \\ (s_{\mathrm{dec},t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \mathrm{if}\ \rho_t = 1 \end{array} \right\} : t = 1, \ldots, L \Big)$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１６３は、以下のように、基底Ｂ*$_0$及び基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の基底ベクトルの係数が設定され、復号要素ｋ*$_{L,dec}$が生成されることを意味する。

まず、基底Ｂ*$_0$の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*$_{0,1}$，．．．，ｂ*$_{0,3}$を意味する。

基底Ｂ*$_0$の基底ベクトル１の係数としてーｓ$_{dec,0}$が設定される。基底ベクトル１＋１，．．．，１＋ｕ$_0$の係数として０が設定される。基底ベクトル１＋ｕ$_0$＋１の係数として１が設定される。基底ベクトル１＋ｕ$_0$＋１＋１，．．．，１＋ｕ$_0$＋１＋ｗ$_0$の係数として$\eta_{dec,0,1}$，．．．，$\eta_{dec,0,wo}$（ここで、ｗ０はｗ$_0$のことである）が設定される。基底ベクトル１＋ｕ$_0$＋１＋ｗ$_0$＋１，．．．，１＋ｕ$_0$＋１＋ｗ$_0$＋ｚ$_0$の係数として０が設定される。

次に、基底Ｂ*$_t$（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ*$_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ*$_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ*

$_{t,1}$，．．．，ｂ＊$_{t,3}$を意味する。また、基底Ｂ＊$_{t}$（ｔ＝１，．．．，Ｌ）については、ρ_tの値が０であるか、１であるかによって場合分けされる。

ρ_tの値が０の場合、基底Ｂ＊$_{t}$（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数として$s_{dec,t}+\theta_{dec,t}v_{t,1}$が設定される。基底ベクトル２，．．．，$n_t$の係数として$\theta_{dec,t}v_{t,2}$，．．．，$\theta_{dec,t}v_{t,nt}$（ここで、ｎｔは$n_t$のことである）が設定される。基底ベクトル$n_t+1$，．．．，$n_t+u_t$の係数として０が設定される。基底ベクトル$n_t+u_t+1$，．．．，$n_t+u_t+w_t$の係数として$\eta_{dec,t,1}$，．．．，$\eta_{dec,t,wt}$（ここで、ｗｔは$w_t$のことである）が設定される。基底ベクトル$n_t+u_t+w_t+1$，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

一方、ρ_tの値が１の場合、基底Ｂ＊$_{t}$（ｔ＝１，．．．，Ｌ）の基底ベクトル１，．．．，n_tの係数として$s_{dec,t}v_{t,1}$，．．．，$s_{dec,t}v_{t,nt}$（ここで、ｎｔはn_tのことである）が設定される。基底ベクトルn_t+1，．．．，n_t+u_tの係数として０が設定される。基底ベクトルn_t+u_t+1，．．．，$n_t+u_t+w_t$の係数として$\eta_{dec,t,1}$，．．．，$\eta_{dec,t,wt}$（ここで、ｗｔはw_tのことである）が設定される。基底ベクトル$n_t+u_t+w_t+1$，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

[0089] （Ｓ６０４：第１ランダム化要素生成ステップ）

ランダム化要素生成部１４３は、処理装置により、ｊ＝１，．．．，２Ｌの各整数ｊについて、復号鍵ｓｋ$_L$の要素である第１ランダム化要素ｋ＊$_{L,ran,j}$を数１６４に示すように生成する。

[数164]

$$k^*_{L,\mathrm{ran},j} := \Big((-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0}, \left\{ \begin{array}{ll} (s_{\mathrm{ran},j,t}\vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathrm{ran},j,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\} : t = 1,\ldots,L \Big)$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ＊とに対して、数１

１１である。したがって、数１６４は、以下のように、基底B^*_0及び基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトルの係数が設定され、第１ランダム化要素$k^*_{L,ran,j}$が生成されることを意味する。

まず、基底B^*_0の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{0,1}$，．．．，$b^*_{0,3}$を意味する。

基底B^*_0の基底ベクトル１の係数として$-s_{ran,j,0}$が設定される。基底ベクトル１＋１，．．．，１＋u_0＋１の係数として０が設定される。基底ベクトル１＋u_0＋１＋１，．．．，１＋u_0＋１＋w_0の係数として$\eta_{ran,j,0,1}$，．．．，$\eta_{ran,j,0,wo}$（ここで、ｗ０はw_0のことである）が設定される。基底ベクトル１＋u_0＋１＋w_0＋１，．．．，１＋u_0＋１＋w_0＋z_0の係数として０が設定される。

次に、基底B^*_t（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{t,1}$，．．．，$b^*_{t,3}$を意味する。また、基底B^*_t（ｔ＝１，．．．，Ｌ）については、ρ_tの値が０であるか、１であるかによって場合分けされる。

ρ_tの値が０の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数として$s_{ran,j,t}+\theta_{ran,j,t}v_{t,1}$が設定される。基底ベクトル２，．．．，$n_t$の係数として$\theta_{ran,j,t}v_{t,2}$，．．．，$\theta_{ran,j,t}v_{t,nt}$（ここで、ｎｔは$n_t$のことである）が設定される。基底ベクトル$n_t$＋１，．．．，$n_t$＋$u_t$の係数として０が設定される。基底ベクトル$n_t$＋$u_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$の係数として$\eta_{ran,j,t,1}$，．．．，$\eta_{ran,j,t,wt}$（ここで、ｗｔは$w_t$のことである）が設定される。基底ベクトル$n_t$＋$u_t$＋$w_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$＋$z_t$の係数として０が設定される。

一方、ρ_tの値が１の場合、基底Ｂ$^*_t$（ｔ＝１，．．．，Ｌ）の基底ベクトル１，．．．，n_tの係数として$s_{ran,j,t}v_{t,1}$，．．．，$s_{ran,j,t}v_{t,n_t}$（ここで、ｎｔはn_tのことである）が設定される。基底ベクトルn_t+1，．．．，n_t+u_tの係数として０が設定される。基底ベクトルn_t+u_t+1，．．．，$n_t+u_t+w_t$の係数として$\eta_{ran,j,t,1}$，．．．，$\eta_{ran,j,t,wt}$（ここで、ｗｔはw_tのことである）が設定される。基底ベクトル$n_t+u_t+w_t+1$，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

[0090] （Ｓ６０５：第２ランダム化要素生成ステップ）

ランダム化要素生成部１４３は、処理装置により、$\tau=L+1$，．．．，ｄの各整数τと、各整数τに関して$\iota=1$，．．．，n_τの各整数ιとについて、復号鍵sk_Lの要素である第２ランダム化要素$k^*_{L,ran,(\tau,\iota,0)}$を数１６５に示すように生成する。

[数165]

$$k^*_{L,\mathrm{ran},(\tau,t,0)} := \Big((-s_{\mathrm{ran},0,0},0^{u_0},0,\vec{\eta}_{\mathrm{ran},0,0},0^{z_0})_{\mathbb{B}^*_0},\ \begin{Bmatrix} (s_{\mathrm{ran},0,t}\vec{e}_{t,1}+\theta_{\mathrm{ran},0,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathrm{ran},0,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0 \\ (s_{\mathrm{ran},0,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathrm{ran},0,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1 \end{Bmatrix} : t=1,\ldots,L),\ (s_{\mathrm{ran},0,L+1}\vec{e}_{\tau,1},0^{u_\tau},\vec{\eta}_{\mathrm{ran},0,(\tau,t)},0^{z_\tau})_{\mathbb{B}^*_\tau} \Big)$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１６５は、以下のように、基底Ｂ$^*_0$と基底Ｂ$^*_t$（ｔ＝１，．．．，Ｌ）と基底Ｂ$^*_\tau$との基底ベクトルの係数が設定され、第２ランダム化要素$k^*_{L,ran,(\tau,\iota,0)}$が生成されることを意味する。

まず、基底Ｂ$^*_0$の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{0,1}$，．．．，$b^*_{0,3}$を

意味する。

基底B^*_0の基底ベクトル１の係数として$-s_{ran,0,0}$が設定される。基底ベクトル１＋１，．．．，１＋u_0＋１の係数として０が設定される。基底ベクトル１＋u_0＋１＋１，．．．，１＋u_0＋１＋w_0の係数として$\eta_{ran,0,0,1}$，．．．，$\eta_{ran,0,0,wo}$（ここで、ｗ０はw_0のことである）が設定される。基底ベクトル１＋u_0＋１＋w_0＋１，．．．，１＋u_0＋１＋w_0＋z_0の係数として０が設定される。

次に、基底B^*_t（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{t,1}$，．．．，$b^*_{t,3}$を意味する。また、基底B^*_t（ｔ＝１，．．．，Ｌ）については、ρ_tの値が０であるか、１であるかによって場合分けされる。

ρ_tの値が０の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数として$s_{ran,0,t}+\theta_{ran,0,t}v_{t,1}$が設定される。基底ベクトル２，．．．，$n_t$の係数として$\theta_{ran,0,t}v_{t,2}$，．．．，$\theta_{ran,0,t}v_{t,nt}$（ここで、ｎｔは$n_t$のことである）が設定される。基底ベクトル$n_t$＋１，．．．，$n_t$＋$u_t$の係数として０が設定される。基底ベクトル$n_t$＋$u_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$の係数として$\eta_{ran,0,t,1}$，．．．，$\eta_{ran,0,t,wt}$（ここで、ｗｔは$w_t$のことである）が設定される。基底ベクトル$n_t$＋$u_t$＋$w_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$＋$z_t$の係数として０が設定される。

一方、ρ_tの値が１の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１，．．．，n_tの係数として$s_{ran,0,t}v_{t,1}$，．．．，$s_{ran,0,t}v_{t,nt}$（ここで、ｎｔはn_tのことである）が設定される。基底ベクトルn_t＋１，．．．，n_t＋u_tの係数として０が設定される。基底ベクトルn_t＋u_t＋１，．．．，n_t＋u_t＋w_tの係数として$\eta_{ran,0,t,1}$，．．．，$\eta_{ran,0,t,wt}$（ここで、ｗｔはw_tのことである）が設定される。基底ベクトルn_t＋u_t＋w_t＋１，．．．，n_t＋u_t＋w_t＋z_tの係数として０が設定される。

次に、基底Ｂ＊$_{\tau}$の部分について説明する。ここでは、表記を簡略化して、基底ベクトルｂ＊$_{\tau,\ i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトルｂ＊$_{\tau,\ 1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトルｂ＊$_{\tau,\ 1}$，．．．，ｂ＊$_{\tau,\ 3}$を意味する。

基底Ｂ＊$_{\tau}$の基底ベクトル１の係数としてｓ$_{ran,\ 0,\ L+1}$が設定される。基底ベクトル２，．．．，ｎ$_{\tau}$，．．．，ｎ$_{\tau}$＋ｕ$_{\tau}$の係数として０が設定される。基底ベクトルｎ$_{\tau}$＋ｕ$_{\tau}$＋１，．．．，ｎ$_{\tau}$＋ｕ$_{\tau}$＋ｗ$_{\tau}$の係数として$\eta_{ran,\ 0,\ (\tau,\ \iota),\ 1}$，．．．，$\eta_{ran,\ 0,\ (\tau,\ \iota)s,\ w\tau}$（ここで、ｗτはｗ$_{\tau}$のことである）が設定される。基底ベクトルｎ$_{\tau}$＋ｕ$_{\tau}$＋ｗ$_{\tau}$＋１，．．．，ｎ$_{\tau}$＋ｕ$_{\tau}$＋ｗ$_{\tau}$＋ｚ$_{\tau}$の係数として０が設定される。

[0091] （Ｓ６０６：第１委譲要素生成ステップ）

委譲要素生成部１４４は、処理装置により、τ＝Ｌ＋１，．．．，ｄの各整数τと、各整数τに関してι＝１，．．．，ｎ$_{\tau}$の各整数ιとについて、復号鍵ｓｋ$_{L}$の要素である第１委譲要素ｋ＊$_{L,\ del,\ (\tau,\ \iota,\ 0)}$を数１６６に示すように生成する。

[数166]

$$
\begin{aligned}
k^{*}_{L,\mathrm{del},(\tau,\iota,0)} := (\ & (-s_{\mathrm{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},0,0}, 0^{z_0})_{\mathbb{B}^{*}_{0}}, \\
& \left\{ \begin{array}{ll} (s_{\mathrm{del},0,t}\vec{e}_{t,1} + \theta_{\mathrm{del},0,t}\vec{v}_{t}, 0^{u_t}, \vec{\eta}_{\mathrm{del},0,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{if } \rho_t = 0 \\ (s_{\mathrm{del},0,t}\vec{v}_{t}, 0^{u_t}, \vec{\eta}_{\mathrm{del},0,t}, 0^{z_t})_{\mathbb{B}^{*}_{t}}, & \text{if } \rho_t = 1 \end{array} \right\} \\
& : t = 1, \ldots, L), \\
& (s_{\mathrm{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},0,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^{*}_{\tau}})
\end{aligned}
$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ＊とに対して、数１１１である。したがって、数１６６は、以下のように、基底Ｂ＊$_{0}$と基底Ｂ＊$_{t}$（ｔ＝１，．．．，Ｌ）と基底Ｂ＊$_{\tau}$との基底ベクトルの係数が設定され、第１委譲要素ｋ＊$_{L,\ del,\ (\tau,\ \iota,\ 0)}$が生成されることを意味する。

まず、基底B^*_0の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{0,1}$，．．．，$b^*_{0,3}$を意味する。

基底B^*_0の基底ベクトル１の係数として$-s_{del,0,0}$が設定される。基底ベクトル１＋１，．．．，１＋u_0＋１の係数として０が設定される。基底ベクトル１＋u_0＋１＋１，．．．，１＋u_0＋１＋w_0の係数として$\eta_{del,0,0,1}$，．．．，$\eta_{del,0,0,wo}$（ここで、ｗ０はw_0のことである）が設定される。基底ベクトル１＋u_0＋１＋w_0＋１，．．．，１＋u_0＋１＋w_0＋z_0の係数として０が設定される。

次に、基底B^*_t（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{t,1}$，．．．，$b^*_{t,3}$を意味する。また、基底B^*_t（ｔ＝１，．．．，Ｌ）については、ρ_tの値が０であるか、１であるかによって場合分けされる。

ρ_tの値が０の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数として$s_{del,0,t}+\theta_{del,0,t}v_{t,1}$が設定される。基底ベクトル２，．．．，$n_t$の係数として$\theta_{del,0,t}v_{t,2}$，．．．，$\theta_{del,0,t}v_{t,nt}$（ここで、ｎｔは$n_t$のことである）が設定される。基底ベクトル$n_t$＋１，．．．，$n_t$＋$u_t$の係数として０が設定される。基底ベクトル$n_t$＋$u_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$の係数として$\eta_{del,0,t,1}$，．．．，$\eta_{del,0,t,wt}$（ここで、ｗｔは$w_t$のことである）が設定される。基底ベクトル$n_t$＋$u_t$＋$w_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$＋$z_t$の係数として０が設定される。

一方、ρ_tの値が１の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１，．．．，n_tの係数として$s_{del,0,t}v_{t,1}$，．．．，$s_{del,0,t}v_{t,nt}$（ここで、ｎｔはn_tのことである）が設定される。基底ベクトルn_t＋１

，．．．．，n_t+u_tの係数として０が設定される。基底ベクトルn_t+u_t+1，．．．，$n_t+u_t+w_t$の係数として$\eta_{del,0,t,1}$，．．．，$\eta_{del,0,t,wt}$（ここで、ｗｔはw_tのことである）が設定される。基底ベクトル$n_t+u_t+w_t+1$，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

次に、基底B^*_τの部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{\tau,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{\tau,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{\tau,1}$，．．．，$b^*_{\tau,3}$を意味する。

基底B^*_τの基底ベクトル１，．．．，n_τの係数として$s_{del,0,L+1}\vec{e}_{\tau,1}+\varphi\vec{e}_{\tau,\iota}$が設定される。基底ベクトル$n_\tau+1$，．．．，$n_\tau+u_\tau$の係数として０が設定される。基底ベクトル$n_\tau+u_\tau+1$，．．．，$n_\tau+u_\tau+w_\tau$の係数として$\eta_{del,0,(\tau,\iota),1}$，．．．，$\eta_{del,0,(\tau,\iota),w\tau}$（ここで、ｗτは$w_\tau$のことである）が設定される。基底ベクトル$n_\tau+u_\tau+w_\tau+1$，．．．，$n_\tau+u_\tau+w_\tau+z_\tau$の係数として０が設定される。

[0092] （Ｓ６０７：第２委譲要素生成ステップ）

委譲要素生成部１４４は、処理装置により、$\tau=L+1$，．．．，ｄの各整数τと、各整数τに関して$\iota=1$，．．．，n_τの各整数ιとについて、復号鍵sk_Lの要素である第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$を数１６７に示すように生成する。

[数167]

$$k^*_{L,\mathrm{del},(\tau,\iota,1)} := \Big((-s_{\mathrm{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},1,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathrm{del},1,t}\vec{e}_{t,1}+\theta_{\mathrm{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \mathrm{if}\ \rho_t=0 \\ (s_{\mathrm{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \mathrm{if}\ \rho_t=1 \end{array} \right\}$$
$$: t=1,\ldots,L),$$
$$(s_{\mathrm{del},1,L+1}\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},1,(\tau,\iota)}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

なお、上述したように、数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。したがって、数１６７は、以下のように、基底B^*_0と基底B^*_t（ｔ＝１，．．．，Ｌ）と基底B^*_τとの基底ベクトルの係数が設定され、第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$が生成されることを意味する。

まず、基底B^*_0の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{0,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{0,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{0,1}$，．．．，$b^*_{0,3}$を意味する。

基底B^*_0の基底ベクトル１の係数として$-s_{del,1,0}$が設定される。基底ベクトル１＋１，．．．，１＋u_0＋１の係数として０が設定される。基底ベクトル１＋u_0＋１＋１，．．．，１＋u_0＋１＋w_0の係数として$\eta_{del,1,0,1}$，．．．，$\eta_{del,1,0,wo}$（ここで、ｗ０はw_0のことである）が設定される。基底ベクトル１＋u_0＋１＋w_0＋１，．．．，１＋u_0＋１＋w_0＋z_0の係数として０が設定される。

次に、基底B^*_t（ｔ＝１，．．．，Ｌ）の部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{t,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{t,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{t,1}$，．．．，$b^*_{t,3}$を意味する。また、基底B^*_t（ｔ＝１，．．．，Ｌ）については、ρ_tの値が０であるか、１であるかによって場合分けされる。

ρ_tの値が０の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１の係数として$s_{del,1,t}+\theta_{del,1,t}v_{t,1}$が設定される。基底ベクトル２，．．．，$n_t$の係数として$\theta_{del,1,t}v_{t,2}$，．．．，$\theta_{del,1,t}v_{t,nt}$（ここで、ｎｔは$n_t$のことである）が設定される。基底ベクトル$n_t$＋１，．．．，$n_t$＋$u_t$の係数として０が設定される。基底ベクトル$n_t$＋$u_t$＋１，．．．，$n_t$＋$u_t$＋$w_t$の係数として$\eta_{del,1,t,1}$，．．．，$\eta_{del,1,t,wt}$（ここで、ｗｔは$w_t$のことである）が設定される。基底ベクトル$n_t$＋$u_t$＋$w_t$

＋１，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

一方、ρ_tの値が１の場合、基底B^*_t（ｔ＝１，．．．，Ｌ）の基底ベクトル１，．．．，n_tの係数として$s_{del,1,t}v_{t,1}$，．．．，$s_{del,1,t}v_{t,nt}$（ここで、ｎｔはn_tのことである）が設定される。基底ベクトルn_t+1，．．．，n_t+u_tの係数として０が設定される。基底ベクトルn_t+u_t+1，．．．，$n_t+u_t+w_t$の係数として$\eta_{del,1,t,1}$，．．．，$\eta_{del,1,t,wt}$（ここで、ｗｔはw_tのことである）が設定される。基底ベクトル$n_t+u_t+w_t+1$，．．．，$n_t+u_t+w_t+z_t$の係数として０が設定される。

次に、基底B^*_τの部分について説明する。ここでは、表記を簡略化して、基底ベクトル$b^*_{\tau,i}$のうち、ｉの部分のみで基底ベクトルを特定する。例えば、基底ベクトル１であれば、基底ベクトル$b^*_{\tau,1}$を意味する。また、基底ベクトル１，．．．，３であれば、基底ベクトル$b^*_{\tau,1}$，．．．，$b^*_{\tau,3}$を意味する。

基底B^*_τの基底ベクトル１，．．．，n_τの係数として$s_{del,1,L+1}\vec{e}_{\tau,\iota}$が設定される。基底ベクトル$n_\tau+1$，．．．，$n_\tau+u_\tau$の係数として０が設定される。基底ベクトル$n_\tau+u_\tau+1$，．．．，$n_\tau+u_\tau+w_\tau$の係数として$\eta_{del,1,(\tau,\iota),1}$，．．．，$\eta_{del,1,(\tau,\iota),w\tau}$（ここで、ｗτは$w_\tau$のことである）が設定される。基底ベクトル$n_\tau+u_\tau+w_\tau+1$，．．．，$n_\tau+u_\tau+w_\tau+z_\tau$の係数として０が設定される。

[0093] （Ｓ６０８：鍵配布ステップ）

鍵配布部１５０は、復号要素$k^*_{L,dec}$と、第１ランダム化要素$k^*_{L,ran,j}$（ｊ＝１，．．．，２Ｌ）と、第２ランダム化要素$k^*_{L,ran,(\tau,\iota,0)}$（τ＝Ｌ＋１，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，n_τ））と、第１委譲要素$k^*_{L,del,(\tau,\iota,0)}$（τ＝Ｌ＋１，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，n_τ））と、第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$（τ＝Ｌ＋１，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，n_τ））とを要素とする復号鍵sk_L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_Lは、他の方法

により復号装置３００へ配布されてもよい。

[0094] つまり、（Ｓ６０１）から（Ｓ６０７）において、鍵生成装置１００は数１６８、数１６９に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵sk_Lを生成する。そして、（Ｓ６０８）で、鍵生成装置１００は生成された復号鍵sk_Lを復号装置３００へ配布する。

[数168]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\rho_1),\ldots,(\vec{v}_L,\rho_L)) := (((v_{1,1},\ldots,v_{1,n_1})\in\mathbb{F}_q^{n_1},\rho_1\in\{0,1\}),\ldots,$$

$$((v_{L,1},\ldots,v_{L,n_L})\in\mathbb{F}_q^{n_L},\rho_L\in\{0,1\})):$$

$$\text{for } j=1,\ldots,2L;\ \tau=L+1,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$

$$\psi,s_{\mathsf{dec},t},s_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q\ (t=1,\ldots,L);$$

$$\theta_{\mathsf{dec},t},\theta_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t},\ \vec{\eta}_{\mathsf{ran},0,t},\ \vec{\eta}_{\mathsf{del},0,t}\ \vec{\eta}_{\mathsf{del},1,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t}\ \ (t=0,\ldots,L);$$

$$s_{\mathsf{ran},0,t},s_{\mathsf{del},0,t},s_{\mathsf{del},1,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q,$$

$$\theta_{\mathsf{ran},0,t},\theta_{\mathsf{del},0,t},\theta_{\mathsf{del},1,t}\xleftarrow{\mathsf{U}}\mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{ran},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},1,(\tau,\iota)}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t}\ ,\ (t=0,\ldots,L+1);$$

$$s_{\mathsf{dec},0}:=\sum_{t=1}^{L}s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},j,t},\ s_{\mathsf{ran},0,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},0,t},$$

$$s_{\mathsf{del},0,0}:=\sum_{t=1}^{L+1}s_{\mathsf{del},0,t},\ s_{\mathsf{del},1,0}:=\sum_{t=1}^{L+1}s_{\mathsf{del},1,t},$$

$$k^*_{L,\mathsf{dec}}:=(\ (-s_{\mathsf{dec},0},0^{u_0},1,\vec{\eta}_{\mathsf{dec},0},0^{z_0})_{\mathbb{B}^*_0},$$

$$\left\{\begin{array}{ll}(s_{\mathsf{dec},t}\vec{e}_{t,1}+\theta_{\mathsf{dec},t},\vec{v}_t,0^{u_t},\vec{\eta}_{\mathsf{dec},t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{dec},t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathsf{dec},t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$

$$:t=1,\ldots,L),$$

$$k^*_{L,\mathsf{ran},j}:=(\ (-s_{\mathsf{ran},j,0},0^{u_0},0,\vec{\eta}_{\mathsf{ran},j,0},0^{z_0})_{\mathbb{B}^*_0},$$

$$\left\{\begin{array}{ll}(s_{\mathsf{ran},j,t}\vec{e}_{t,1}+\theta_{\mathsf{ran},j,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathsf{ran},j,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{ran},j,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathsf{ran},j,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$

$$:t=1,\ldots,L),$$

[数169]

$$k^*_{L,\mathsf{ran},(\tau,t,0)} := ((-s_{\mathsf{ran},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},0,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{ran},0,L+1}\vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,0)} := ((-s_{\mathsf{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},0,t}\vec{e}_{t,1} + \theta_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,1)} := ((-s_{\mathsf{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},1,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},1,t}\vec{e}_{t,1} + \theta_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{del},1,L+1}\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},1,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (((\vec{v}_1, \rho_1), \ldots, (\vec{v}_L, \rho_L));$$
$$k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L}, \{k^*_{L,\mathsf{ran},(\tau,t,0)}, k^*_{L,\mathsf{del},(\tau,t,0)}, k^*_{L,\mathsf{del},(\tau,t,1)}\}$$
$$\tau = L+1, \ldots, d; (\tau,t) = (\tau,1), \ldots, (\tau,n_\tau)),$$

return sk_L.

[0095] 図１８に基づき、復号装置３００が実行するＤｅｃアルゴリズムの処理について説明する。

（Ｓ７０１：復号鍵取得ステップ）

復号鍵取得部３１０は、例えば、通信装置によりネットワークを介して、復号鍵ｓｋ$_L$を取得する。また、復号鍵取得部３１０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。

[0096] （Ｓ７０２：データ受信ステップ）

データ受信部３２０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が送信した暗号化データｃｔを受信する。

[0097] （Ｓ７０３：ペアリング演算ステップ）

ペアリング演算部３３０は、処理装置により、数１７０に示すペアリング演算を行い、セッション鍵Ｋ＝g_T^{ζ}を計算する。

[数170]

$$K := e(c_{1,0}, k^*_{L,\mathrm{dec},0}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 0} e(c_{1,t}, k^*_{L,\mathrm{dec},t}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 1} e(c_{1,t}, k^*_{L,\mathrm{dec},t})^{1/(\vec{v}_t \cdot \vec{x}_t)}$$

ここで、数１７１である。

[数171]

$$(k^*_{L,\mathrm{dec},0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, k^*_{L,\mathrm{dec},d} \in \langle \mathbb{B}^*_d \rangle) := k^*_{L,\mathrm{dec}},$$
$$(c_{1,0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, c_{1,d} \in \langle \mathbb{B}^*_d \rangle := c_1$$

なお、ｔ＝１，．．．，Ｌの各整数ｔに関して、ρ_t＝０の整数ｔについて$\vec{v}_t$と$\vec{x}_t$との内積が０であり、ρ_t＝１の整数ｔについて$\vec{v}_t$と$\vec{x}_t$との内積が０でなければ、数１７０を計算することにより、セッション鍵Ｋが計算される。

[0098] （Ｓ７０４：メッセージ計算ステップ）

メッセージ計算部３４０は、処理装置により、暗号化データｃ２をセッション鍵Ｋで割ることにより、メッセージｍ’（＝ｍ）を計算する。

[0099] つまり、（Ｓ７０１）から（Ｓ７０４）において、復号装置３００は数１７２に示すＤｅｃアルゴリズムを実行して、メッセージｍ’（＝ｍ）を計算する。

[数172]

$$\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_L, \mathrm{ct}):$$
$$K := e(c_{1,0}, k^*_{L,\mathrm{dec},0}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 0} e(c_{1,t}, k^*_{L,\mathrm{dec},t}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 1} e(c_{1,t}, k^*_{L,\mathrm{dec},t})^{1/(\vec{v}_t \cdot \vec{x}_t)},$$
$$\text{where } (k^*_{L,\mathrm{dec},0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, k^*_{L,\mathrm{dec},d} \in \langle \mathbb{B}^*_d \rangle) := k^*_{L,\mathrm{dec}},$$
$$(c_{1,0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, c_{1,d} \in \langle \mathbb{B}^*_d \rangle := c_1,$$
$$m' := c_2 / K,$$
$$\text{return } m'.$$

[0100] 図１９に基づき、鍵委譲装置４００が実行するＤｅｌｅｇａｔｅ$_L$アルゴリズムの処理について説明する。

（Ｓ８０１：復号鍵取得ステップ）

復号鍵取得部４１０は、例えば、通信装置によりネットワークを介して、復号鍵ｓｋ$_L$を取得する。また、復号鍵取得部４１０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。

[0101] （Ｓ８０２：情報入力ステップ）

情報入力部４２０は、入力装置により、述語情報（$\vec{v}_{L+1}$，ρ_{L+1}）：＝（$v_{L+1,i}$（ｉ＝１，．．．，n_{L+1}），$\rho_{L+1} \in \{0, 1\}$）を入力する。なお、述語情報としては、鍵を委譲される者の属性が入力される。

[0102] （Ｓ８０３：乱数生成ステップ）

乱数生成部４３１は、処理装置により、ｊ＝１，．．．，２Ｌと，ｊ’＝１，．．．，２（Ｌ＋１）と，τ＝Ｌ＋２，．．．，ｄと，（τ，ι）＝（τ，１），．．．，（τ，n_τ）と，ｔ＝０，．．．，Ｌ＋１，τと，（ｔ，ｉ）＝（ｔ，１），．．．，（ｔ，n_t）との各整数ｊ，ｊ’，τ，ι，ｔ，ｉについて、乱数$\alpha_{\mathrm{dec},j}$，σ_{dec}，$\alpha_{\mathrm{ran},j',j}$，$\sigma_{\mathrm{ran},j'}$，$\alpha_{\mathrm{ran},(\tau,\iota,0),j}$，$\sigma_{\mathrm{ran},(\tau,\iota,0)}$，$\phi_{\mathrm{ran},(\tau,\iota,0)}$，$\alpha_{\mathrm{del},(\tau,\iota,0),j}$，$\sigma_{\mathrm{del},(\tau,\iota,0)}$，$\phi_{\mathrm{del},(\tau,\iota,0)}$，$\alpha_{\mathrm{del},(\tau,\iota,1),j}$，$\sigma_{\mathrm{del},(\tau,\iota,1)}$，$\phi_{\mathrm{del},(\tau}$

, ι, 1)，$\eta_{dec,(t,i)}$，$\eta_{ran,j',(t,i)}$，$\eta_{ran,(\tau,\iota,0),(t,i)}$，$\eta_{del,(\tau,\iota,0),(t,i)}$，$\eta_{del,(\tau,\iota,1),(t,i)}$，$\psi_0$，$\psi_1$を数１７３に示すように生成する。

[数173]

$$\text{for } j=1,...,2L;\ j'=1,...,2(L+1);\ \tau=L+2,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$$
$$t=0,...,L+1,\tau;\ (t,i)=(t,1),...,(t,w_t);$$
$$\alpha_{\mathrm{dec},j},\ \sigma_{\mathrm{dec}},\ \alpha_{\mathrm{ran},j',j},\ \sigma_{\mathrm{ran},j'},\ \alpha_{\mathrm{ran},(\tau,\iota,0),j},\ \sigma_{\mathrm{ran},(\tau,\iota,0)},$$
$$\phi_{\mathrm{ran},(\tau,\iota,0)},\ \alpha_{\mathrm{del},(\tau,\iota,0),j},\ \sigma_{\mathrm{del},(\tau,\iota,0)},\ \phi_{\mathrm{del},(\tau,\iota,0)},\ \alpha_{\mathrm{del},(\tau,\iota,1),j},$$
$$\sigma_{\mathrm{del},(\tau,\iota,1)},\ \phi_{\mathrm{del},(\tau,\iota,1)},\ \eta_{\mathrm{dec},(t,i)},\ \eta_{\mathrm{ran},j',(t,i)},\ \eta_{\mathrm{ran},(\tau,\iota,0),(t,i)},$$
$$\eta_{\mathrm{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathrm{del},(\tau,\iota,1),(t,i)},\ \psi_0,\psi_1,\xleftarrow{U}\mathbb{F}_q$$

[0103] （Ｓ８０４：下位復号要素生成ステップ）

下位復号要素生成部４３２は、処理装置により、委譲鍵ｓｋ$_{L+1}$の要素である下位復号要素ｋ*$_{L+1,dec}$を数１７４に示すように生成する。

[数174]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L}\alpha_{\mathrm{dec},j}k^*_{L,\mathrm{ran},j}$$
$$+\left\{\begin{array}{ll}(\sigma_{\mathrm{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ (\sigma_{\mathrm{dec}}([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad +\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathrm{del},(L+1,i,1)}]_L) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathrm{dec},(0,i)}b^*_{0,1+u_0+1+i}+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathrm{dec},(t,i)}b^*_{t,n_t+u_t+i}$$

[0104] （Ｓ８０５：第１下位ランダム化要素生成ステップ）

下位ランダム化要素生成部４３３は、処理装置により、ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’について、委譲鍵ｓｋ$_{L+1}$の要素である第１下位ランダム化要素ｋ*$_{L+1,ran,j'}$を数１７５に示すように生成する。

[数175]

$$k^{*}_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},j',j} k^{*}_{L,\mathrm{ran},j} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},j'}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)}\right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{ran},j'}\left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} + \sum_{i=1}^{n_{L+1}} v_{L+1,i}[k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}\right) & \text{if } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^{*}_{t,n_t+u_t+i}$$

[0105] （Ｓ８０６：第２下位ランダム化要素生成ステップ）

下位ランダム化要素生成部４３３は、処理装置により、τ＝Ｌ＋２，．．．，ｄの各整数τと、各整数τについてι＝１，．．．．，n_τの各整数ιについて、委譲鍵sk_{L+1}の要素である第２下位ランダム化要素$k^{*}_{L+1,\mathrm{ran},(\tau,\iota)}$を数１７６に示すように生成する。

[数176]

$$k^{*}_{L+1,\mathrm{ran},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota)j,} k^{*}_{L,\mathrm{ran},j} + \phi_{\mathrm{ran},(\tau,\iota,0)} k^{*}_{L,\mathrm{ran},(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},(\tau,\iota,0)}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)}\right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{ran},(\tau,\iota,0)}\left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} + \sum_{i=1}^{n_{L+1}} v_{L+1,i}[k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}\right) & \text{if } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^{*}_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^{*}_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

[0106] （Ｓ８０７：第１下位委譲要素生成ステップ）

下位委譲要素生成部４３４は、処理装置により、τ＝Ｌ＋２，．．．，ｄ

の各整数τと、各整数τについてι＝１，．．．．，ｎ$_{\tau}$の各整数ιとについて、委譲鍵ｓｋ$_{L+1}$の要素である第１下位委譲要素ｋ*$_{L+1,del,(\tau,\iota,0)}$を数１７７に示すように生成する。

[数177]

$$k^*_{L+1,\mathrm{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^*_{L,\mathrm{ran}(\tau,\iota,0)} + \psi_0 k^*_{L,\mathrm{del}(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,0)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)} \right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} \left([k^*_{L,\mathrm{del},(L+1,i,1)}]^L \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{if } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

[0107] （Ｓ８０８：第２下位委譲要素生成ステップ）

下位委譲要素生成部４３４は、処理装置により、τ＝Ｌ＋２，．．．，ｄの各整数τと、各整数τについてι＝１，．．．．，ｎ$_{\tau}$の各整数ιとについて、委譲鍵ｓｋ$_{L+1}$の要素である第２下位委譲要素ｋ*$_{L+1,del,(\tau,\iota,1)}$を数１７８に示すように生成する。

[数178]

$$k^*_{L+1,\mathrm{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^*_{L,\mathrm{ran},j} + \psi_1 k^*_{L,\mathrm{del}(\tau,\iota,1)}$$
$$+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,1)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \qquad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

[0108] （Ｓ８０９：鍵配布ステップ）

鍵配布部１５０は、下位復号要素ｋ*$_{L+1,\mathrm{dec}}$と、第１下位ランダム化要素ｋ*$_{L+1,\mathrm{ran},j'}$（ｊ’＝１，．．．，２（Ｌ＋１））と、第２下位ランダム化要素ｋ*$_{L+1,\mathrm{ran},(\tau,\iota,0)}$（τ＝Ｌ＋２，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，ｎ$_\tau$））と、第１下位委譲要素ｋ*$_{L+2,\mathrm{del},(\tau,\iota,0)}$（τ＝Ｌ＋２，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，ｎ$_\tau$））と、第２下位委譲要素ｋ*$_{L+2,\mathrm{del},(\tau,\iota,1)}$（τ＝Ｌ＋２，．．．，ｄ；（τ，ι）＝（τ，１），．．．，（τ，ｎ$_\tau$））とを要素とする委譲鍵ｓｋ$_{L+1}$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下位の復号装置３００へ配布する。もちろん、委譲鍵ｓｋ$_{L+1}$は、他の方法により下位の復号装置３００へ配布されてもよい。

[0109] つまり、（Ｓ５０１）から（Ｓ５０７）において、鍵委譲装置４００は数１７９、数１８０に示すＤｅｌｅｇａｔｅ$_L$アルゴリズムを実行して、委譲鍵ｓｋ$_{L+1}$を生成する。そして、（Ｓ５０８）で、鍵委譲装置４００は生成された委譲鍵ｓｋ$_{L+1}$を下位の復号装置３００へ配布する。

[数179]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,(\vec{v}_{L+1},\rho_{L+1}):=((v_{L+1,1},...,v_{L+1,n_{L+1}}),\rho_{L+1})):$$

for $j=1,...,2L;\ j'=1,...,2(L+1);\ \tau=L+2,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$

$t=0,...,L+1,\tau;\ (t,i)=(t,1),...,(t,w_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota,0),j},\ \sigma_{\mathsf{ran},(\tau,\iota,0)},\ \phi_{\mathsf{ran},(\tau,\iota,0)},$

$\alpha_{\mathsf{del},(\tau,\iota,0),j},\ \sigma_{\mathsf{del},(\tau,\iota,0)},\ \phi_{\mathsf{del},(\tau,\iota,0)},\ \alpha_{\mathsf{del},(\tau,\iota,1),j},\ \sigma_{\mathsf{del},(\tau,\iota,1)},\ \phi_{\mathsf{del},(\tau,\iota,1)},$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,1),(t,i)},$

$\psi_0,\psi_1,\xleftarrow{\cup}\mathbb{F}_q,$

$$k^*_{L+1,\mathsf{dec}}:=k^*_{L,\mathsf{dec}}+\sum_{j=1}^{2L}\alpha_{\mathsf{dec},j}k^*_{L,\mathsf{ran},j}$$
$$+\left\{\begin{array}{ll}(\sigma_{\mathsf{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ (\sigma_{\mathsf{dec}}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(0,i)}b^*_{0,1+u_0+1+i}+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},j'}:=\sum_{j=1}^{2L}\alpha_{\mathsf{ran},j',j}k^*_{L,\mathsf{ran},j}$$
$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},j'}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ \sigma_{\mathsf{ran},j'}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(0,i)}b^*_{0,1+u_0+1+i}$$
$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},(\tau,\iota,0)}:=\sum_{j=1}^{2L}\alpha_{\mathsf{ran},(\tau,\iota)j,}k^*_{L,\mathsf{ran},j}+\phi_{\mathsf{ran},(\tau,\iota,0)}k^*_{L,\mathsf{ran},(\tau,\iota,0)}$$
$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},(\tau,\iota,0)}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ \sigma_{\mathsf{ran},(\tau,\iota,0)}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(0,i)}b^*_{0,1+u_0+1+i}$$
$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(t,i)}b^*_{t,n_t+u_t+i}$$
$$+\sum_{i=1}^{w_\tau}\eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)}b^*_{\tau,n_\tau+u_\tau+i},$$

[数180]

$$
\begin{aligned}
k^*_{L+1,\mathrm{del},(\tau,\iota,0)} :=& \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^*_{L,\mathrm{ran}(\tau,\iota,0)} \\
&+ \psi_0 k^*_{L,\mathrm{del}(\tau,\iota,0)} \\
&+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,0)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \qquad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\} \\
&+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^*_{0,1+u_0+1+i} \\
&+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,n_t+u_t+i} \\
&+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}, \\
k^*_{L+1,\mathrm{del},(\tau,\iota,1)} :=& \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^*_{L,\mathrm{ran},j} + \psi_1 k^*_{L,\mathrm{del}(\tau,\iota,1)} \\
&+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,1)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \qquad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\} \\
&+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(0,i)} b^*_{0,1+u_0+1+i} \\
&+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^*_{t,n_t+u_t+i} \\
&+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}, \\
\mathrm{sk}_{L+1} :=& (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_{L+1},\rho_{L+1})); \\
& k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)}, \\
& \{k^*_{L+1,\mathrm{ran},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,1)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}), \\
& \text{return } \mathrm{sk}_{L+1}.
\end{aligned}
$$

[0110] なお、下位の復号装置３００が、委譲鍵ｓｋ$_{L+1}$を用いてＤｅｃアルゴリズムを実行した場合、図１５の（Ｓ４０３）では、（ｖ$^{\rightarrow}_1$，．．．，ｖ$^{\rightarrow}_{L+1}$）と（ｘ$^{\rightarrow}_1$，．．．，ｘ$^{\rightarrow}_{L+1}$）との内積が０であれば、数１７０を計算することにより、セッション鍵Ｋが計算される。

[0111] 以上のように、実施の形態２に係る暗号処理システム１０は、一部については属性情報と述語情報との内積が０となり、残りの部分については属性情

報と述語情報との内積が０とならない場合に、復号可能な階層的内積述語暗号方式を実現する。そのため、例えば、肯定形と否定形との条件設定などが可能である。

[0112] なお、上記説明において、u_t、w_t、z_t（t＝0，．．．，d）の次元は、安全性を高めるために設けた次元である。したがって、安全性が低くなってしまうが、u_t、w_t、z_t（t＝0，．．．，d）をそれぞれ０として、u_t、w_t、z_t（t＝0，．．．，d）の次元を設けなくてもよい。

[0113] また、上記説明では、N_0に$1+u_0+1+w_0+z_0$を設定し、N_tに$n_t+u_t+w_t+z_t$を設定した。しかし、$1+u_0+1+w_0+z_0$を$1+1+1+1+1$としてN_0に５を設定し、$n_t+u_t+w_t+z_t$を$n_t+n_t+n_t+1$としてN_tに$3n_t+1$を設定してもよい。

この場合、数１６８、数１６９に示すＫｅｙＧｅｎアルゴリズムは、数１８１、数１８２のように書き換えられる。

[数181]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\rho_1),...,(\vec{v}_L,\rho_L)) := (((v_{1,1},...,v_{1,n_1}) \in \mathbb{F}_q^{n_1}, \rho_1 \in \{0,1\}),...,$$

$$((v_{L,1},...,v_{L,n_L}) \in \mathbb{F}_q^{n_L}, \rho_L \in \{0,1\})):$$

for $j = 1,...,2L;\ \tau = L+1,...,d;\ (\tau,\iota) = (\tau,1),...,(\tau,n_\tau);$

$$\psi, s_{\mathsf{dec},t}, s_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q \ (t = 1,...,L);$$

$$\theta_{\mathsf{dec},t}, \theta_{\mathsf{ran},j,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t},\ \vec{\eta}_{\mathsf{ran},0,t},\ \vec{\eta}_{\mathsf{del},0,t}\ \vec{\eta}_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t} \ (t = 0,...,L);$$

$$s_{\mathsf{ran},0,t}, s_{\mathsf{del},0,t}, s_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\theta_{\mathsf{ran},0,t}, \theta_{\mathsf{del},0,t}, \theta_{\mathsf{del},1,t} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$

$$\vec{\eta}_{\mathsf{ran},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},0,(\tau,\iota)},\ \vec{\eta}_{\mathsf{del},1,(\tau,\iota)} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{n_t}\ , (t = 0,...,L+1);$$

$$s_{\mathsf{dec},0} := \sum_{t=1}^{L} s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0} := \sum_{t=1}^{L} s_{\mathsf{ran},j,t},\ s_{\mathsf{ran},0,0} := \sum_{t=1}^{L} s_{\mathsf{ran},0,t},$$

$$s_{\mathsf{del},0,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},0,t},\ s_{\mathsf{del},1,0} := \sum_{t=1}^{L+1} s_{\mathsf{del},1,t},$$

$$k^*_{L,\mathsf{dec}} := (\ (-s_{\mathsf{dec},0}, 0, 1, \eta_{\mathsf{dec},0}, 0)_{\mathbb{B}^*_0},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{dec},t}\ \vec{e}_{t,1} + \theta_{\mathsf{dec},t}, \vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{dec},t}, 0)_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{dec},t}\ \vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{dec},t}, 0)_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\} : t = 1,...,L),$$

$$k^*_{L,\mathsf{ran},j} := (\ (-s_{\mathsf{ran},j,0}, 0, 0, \eta_{\mathsf{ran},j,0}, 0)_{\mathbb{B}^*_0},$$

$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{ran},j,t}, 0)_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{ran},j,t}\ \vec{v}_t, 0^{n_t},\ \vec{\eta}_{\mathsf{ran},j,t}, 0)_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$

$$: t = 1,...,L),$$

[数182]

$$k^*_{L,\mathsf{ran},(\tau,\iota,0)} := ((-s_{\mathsf{ran},0,0},0,0,\eta_{\mathsf{ran},0,0},0)_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathsf{ran},0,t}\,\vec{e}_{t,1}+\theta_{\mathsf{ran},0,t}\vec{v}_t,0^{n_t},\vec{\eta}_{\mathsf{ran},0,t},0)_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{ran},0,t}\,\vec{v}_t,0^{n_t},\vec{\eta}_{\mathsf{ran},0,t},0)_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$
$$: t=1,\ldots,L),$$
$$(s_{\mathsf{ran},0,L+1}\,\vec{e}_{\tau,1},0^{n_\tau},\vec{\eta}_{\mathsf{ran},0,(\tau,\iota)},0)_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,\iota,0)} := ((-s_{\mathsf{del},0,0},0,0,\eta_{\mathsf{del},0,0},0)_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathsf{del},0,t}\,\vec{e}_{t,1}+\theta_{\mathsf{del},0,t}\vec{v}_t,0^{n_t},\vec{\eta}_{\mathsf{del},0,t},0)_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{del},0,t}\,\vec{v}_t,0^{n_t},\vec{\eta}_{\mathsf{del},0,t},0)_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$
$$: t=1,\ldots,L),$$
$$(s_{\mathsf{del},0,L+1}\,\vec{e}_{\tau,1},+\psi\vec{e}_{\tau,\iota},0^{n_\tau},\vec{\eta}_{\mathsf{del},0,(\tau,\iota)},0)_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,\iota,1)} := ((-s_{\mathsf{del},1,0},0,0,\eta_{\mathsf{del},1,0},0)_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathsf{del},1,t}\,\vec{e}_{t,1}+\theta_{\mathsf{del},1,t}\vec{v}_t,0^{n_t},\vec{\eta}_{\mathsf{del},1,t},0)_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{del},1,t}\,\vec{v}_t,0^{n_t},\vec{\eta}_{\mathsf{del},1,t},0)_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$
$$: t=1,\ldots,L),$$
$$(s_{\mathsf{del},1,L+1}\,\vec{e}_{\tau,\iota},0^{n_\tau},\vec{\eta}_{\mathsf{del},1,(\tau,\iota)},0)_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_L,\rho_L));$$
$$k^*_{L,\mathsf{dec}},\{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L},\{k^*_{L,\mathsf{ran},(\tau,\iota,0)},k^*_{L,\mathsf{del},(\tau,\iota,0)},k^*_{L,\mathsf{del},(\tau,\iota,1)}\}$$
$$\tau=L+1,\ldots,d;(\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)),$$

return sk_L.

また、数１７９、数１８０に示すＤｅｌｅｇａｔｅ$_L$アルゴリズムは、数１８３、数１８４のように書き換えられる。

[数183]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,(\vec{v}_{L+1},\rho_{L+1}):=((v_{L+1,1},...,v_{L+1,n_{L+1}}),\rho_{L+1})):$$

for $j=1,...,2L;\ j'=1,...,2(L+1);\ \tau=L+2,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau);$

$t=0,...,L+1,\tau;\ (t,i)=(t,1),...,(t,n_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota,0),j},\ \sigma_{\mathsf{ran},(\tau,\iota,0)},\ \phi_{\mathsf{ran},(\tau,\iota,0)},$

$\alpha_{\mathsf{del},(\tau,\iota,0),j},\ \sigma_{\mathsf{del},(\tau,\iota,0)},\ \phi_{\mathsf{del},(\tau,\iota,0)},\ \alpha_{\mathsf{del},(\tau,\iota,1),j},\ \sigma_{\mathsf{del},(\tau,\iota,1)},\ \phi_{\mathsf{del},(\tau,\iota,1)},$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,1),(t,i)},$

$\psi_0,\psi_1,\xleftarrow{\cup}\mathbb{F}_q,$

$$k^*_{L+1,\mathsf{dec}}:=k^*_{L,\mathsf{dec}}+\sum_{j=1}^{2L}\alpha_{\mathsf{dec},j}k^*_{L,\mathsf{ran},j}$$
$$+\left\{\begin{array}{ll}(\sigma_{\mathsf{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ (\sigma_{\mathsf{dec}}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\eta_{\mathsf{dec},(0,1)}b^*_{0,4}+\sum_{t=1}^{L+1}\sum_{i=1}^{n_t}\eta_{\mathsf{dec},(t,i)}b^*_{t,2n_t+i},$$

$$k^*_{L+1,\mathsf{ran},j'}:=\sum_{j=1}^{2L}\alpha_{\mathsf{ran},j',j}k^*_{L,\mathsf{ran},j}$$
$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},j'}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ \sigma_{\mathsf{ran},j'}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\eta_{\mathsf{ran},j',(0,1)}b^*_{0,4}+\sum_{t=1}^{L+1}\sum_{i=1}^{n_t}\eta_{\mathsf{ran},j',(t,i)}b^*_{t,2n_t+i},$$

$$k^*_{L+1,\mathsf{ran},(\tau,\iota,0)}:=\sum_{j=1}^{2L}\alpha_{\mathsf{ran},(\tau,\iota)j,}k^*_{L,\mathsf{ran},j}+\phi_{\mathsf{ran},(\tau,\iota,0)}k^*_{L,\mathsf{ran},(\tau,\iota,0)}$$
$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},(\tau,\iota,0)}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ \sigma_{\mathsf{ran},(\tau,\iota,0)}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\eta_{\mathsf{del},(\tau,\iota,0),(0,1)}b^*_{0,4}+\sum_{t=1}^{L+1}\sum_{i=1}^{n_t}\eta_{\mathsf{del},(\tau,\iota,0),(t,i)}b^*_{t,2n_t+i}$$
$$+\sum_{i=1}^{n_\tau}\eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)}b^*_{\tau,2n_\tau+i},$$

[数184]

$$k^*_{L+1,\mathrm{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^*_{L,\mathrm{ran}(\tau,\iota,0)}$$
$$+ \psi_0 k^*_{L,\mathrm{del}(\tau,\iota,0)}$$
$$+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,0)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\}$$
$$+ \eta_{\mathrm{del},(\tau,\iota,0),(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,2n_t+i}$$
$$+ \sum_{i=1}^{n_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,2n_\tau+i},$$
$$k^*_{L+1,\mathrm{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^*_{L,\mathrm{ran},j} + \psi_1 k^*_{L,\mathrm{del}(\tau,\iota,1)}$$
$$+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,1)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\}$$
$$+ \eta_{\mathrm{del},(\tau,\iota,1),(0,1)} b^*_{0,4} + \sum_{t=1}^{L+1} \sum_{i=1}^{n_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^*_{t,2n_t+i}$$
$$+ \sum_{i=1}^{n_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,2n_\tau+i},$$
$$\mathsf{sk}_{L+1} := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_{L+1},\rho_{L+1}));$$
$$k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathrm{ran},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,1)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$
return sk_{L+1}.

なお、数１７２に示すＤｅｃアルゴリズムに変更はない。

[0114] また、Ｓｅｔｕｐアルゴリズムは、暗号処理システム１０のセットアップ時に一度実行すればよく、復号鍵を生成する度に実行する必要はない。また、上記説明では、ＳｅｔｕｐアルゴリズムとＫｅｙＧｅｎアルゴリズムとを鍵生成装置１００が実行するとしたが、ＳｅｔｕｐアルゴリズムとＫｅｙＧｅｎアルゴリズムとをそれぞれ異なる装置が実行するとしてもよい。

[0115] 実施の形態３．

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。この実施の形態では、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。

[0116] 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処理を実現した。しかし、合成数Ｍを用いて数１８５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185]

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

ここで、
$\mathbb{Z}$ ：整数
M ：合成数
である。

[0117] 実施の形態１で説明した階層的述語暗号方式を、環Ｒを係数とする加群において実現すると数１８６から数１９３のようになる。

[数186]

$$\begin{aligned}
&\mathsf{Setup}(1^{\lambda}, \vec{n} := (d; n_1,...,n_d, u_0,...,u_d, w_0,...,w_d, z_0,...,z_d)):\\
&\quad (\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,...,d}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^{\lambda}, \vec{n}),\\
&\quad \hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,1+u_0+1}, b_{0,1+u_0+1+w_0+1},..., b_{0,1+u_0+1+w_0+z_0}),\\
&\quad \hat{\mathbb{B}}_t := (b_{t,1},.., b_{t,n_t}, b_{t,n_t+u_t+w_t+1},..., b_{t,n_t+u_t+w_t+z_t}) \quad \text{for } t=1,..,d,\\
&\quad \hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,1+u_0+1}^*),\\
&\quad \hat{\mathbb{B}}_t^* := (b_{t,1}^*,.., b_{t,n_t}^*) \quad \text{for } t=1,..,d,\\
&\quad \mathsf{pk} := (1^{\lambda}, \mathsf{param}_{\vec{n}}, \{\hat{\mathbb{B}}_t\}_{t=0,...,d},\\
&\qquad\quad b_{0,1+u_0+1+1},..., b_{0,1+u_0+1+w_0}^*, \{b_{t,n_t+u_t+1}^*,..., b_{t,n_t+u_t+w_t}^*\}_{t=1,...,d}),\\
&\quad \mathsf{sk} := \{\hat{\mathbb{B}}_t^*\}_{t=0,...,d},\\
&\quad \text{return pk, sk.}
\end{aligned}$$

[数187]

$$\mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}:=(d;\vec{n}:=(d;n_1,...,n_d,u_0,...,u_d,w_0,...,w_d,z_0,...,z_d)$$

$$N_0:=1+u_0+1+w_0+z_0,\ N_t:=n_t+u_t+w_t+z_t \quad \text{for } t=1,..,d,$$

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

$$\psi\xleftarrow{\mathsf{U}}\mathbb{R}^{\times},$$

For $t=0,\ldots,d$,

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

$$X_t:=(\chi_{t,i,j})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t,\mathbb{R}),\quad (\nu_{t,i,j})_{i,j}:=\psi\cdot(X_t^{\mathrm{T}})^{-1},$$

$$b_{t,i}:=(\chi_{t,i,1},\ldots,\chi_{t,i,N_t})_{\mathbb{A}_t}=\sum_{j=1}^{N_t}\chi_{t,i,j}a_{t,j},\ \mathbb{B}_t:=(b_{t,1},\ldots,b_{t,N_t}),$$

$$b^*_{t,i}:=(\nu_{t,i,1},\ldots,\nu_{t,i,N_t})_{\mathbb{A}_t}=\sum_{j=1}^{N_t}\nu_{t,i,j}a_{t,j},\ \mathbb{B}^*_t:=(b^*_{t,1},\ldots,b^*_{t,N_t}),$$

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

return $(\mathsf{param}^{-}_{n},\{\mathbb{B}_t,\mathbb{B}^*_t\}_{t=0,\ldots,d})$.

[数188]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,...,\vec{v}_L):=(v_{1,1},...,v_{1,n_1}),...,\ (v_{L,1},...,v_{L,n_L})):$$

for $j=1,...,2L;\ \tau=L+1,...,d;\ (\tau,\iota)=(\tau,1),...,(\tau,n_\tau)$;

$$\psi,s_{\mathsf{dec},t},s_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{R}\ (t=1,...,L);$$

$$\theta_{\mathsf{dec},t},\theta_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{R},\ \vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t}\ (t=0,...,L);$$

$$s_{\mathsf{ran},(\tau,\iota),t},s_{\mathsf{del},(\tau,\iota),t}\xleftarrow{\mathsf{U}}\mathbb{R}\ (t=1,...,L+1);$$

$$\theta_{\mathsf{ran},(\tau,\iota),t},\theta_{\mathsf{del},(\tau,\iota),t}\xleftarrow{\mathsf{U}}\mathbb{R},\ \vec{\eta}_{\mathsf{ran},(\tau,\iota),t},\ \vec{\eta}_{\mathsf{del},(\tau,\iota),t}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t},$$
$$(t=0,...,L+1);$$

$$s_{\mathsf{dec},0}:=\sum_{t=1}^{L}s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},j,t},$$

$$s_{\mathsf{ran},(\tau,\iota),0}:=\sum_{t=1}^{L+1}s_{\mathsf{ran},(\tau,\iota),t},\ s_{\mathsf{del},(\tau,\iota),0}:=\sum_{t=1}^{L+1}s_{\mathsf{del},(\tau,\iota),t},$$

[数189]

$$k^*_{L,\mathsf{dec}} := ((-s_{\mathsf{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathsf{dec},0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{dec},t}\ \vec{e}_{t,1} + \theta_{\mathsf{dec},t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{dec},t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L),$$
$$k^*_{L,\mathsf{ran},j} := ((-s_{\mathsf{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L),$$
$$k^*_{L,\mathsf{ran},(\tau,t)} := ((-s_{\mathsf{ran},(\tau,t),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},(\tau,t),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{ran},(\tau,t),t}\ \vec{e}_{t,1} + \theta_{\mathsf{ran},(\tau,t),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{ran},(\tau,t),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathsf{ran},(\tau,t),L+1}\ \vec{e}_{\tau,1},\ 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},(\tau,t),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$
$$k^*_{L,\mathsf{del},(\tau,t)} := ((-s_{\mathsf{del},(\tau,t),0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},(\tau,t),0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$(s_{\mathsf{del},(\tau,t),t}\ \vec{e}_{t,1} + \theta_{\mathsf{del},(\tau,t),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathsf{del},(\tau,t),t}, 0^{z_t})_{\mathbb{B}^*_t}$$
$$: t = 1,\ldots,L$$
$$(s_{\mathsf{del},(\tau,t),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},(\tau,t),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$
$$\mathsf{sk}_L := (k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L},$$
$$\{k^*_{L,\mathsf{ran},(\tau,t)}\}_{\tau=L+1,\ldots,d;\ (\tau,t)=(\tau,1),\ldots,(\tau,n_\tau)},$$
$$\{k^*_{L,\mathsf{del},(\tau,t)}\}_{\tau=L+1,\ldots,d;\ (\tau,t)=(\tau,1),\ldots,(\tau,n_\tau)}),$$
return sk_L.

[数190]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$
$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\mathsf{U}} \mathbb{R}^{n_{L+1}} \times \cdots \times \mathbb{R}^{n_d};$$
$$\omega, \zeta \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\varphi}_t \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t}\ (t = 0,\ldots,d),$$
$$c_1 := ((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1,\ldots,d),$$
$$c_2 := g_T^{\zeta} m,$$
$$\mathsf{ct} := (c_1, c_2),$$
return ct.

[数191]

$$\mathsf{Dec}(\mathsf{pk}, k^*_{L,\mathsf{dec}}, \mathsf{ct}):\ m' := c_2 / e(c_1, k^*_{L,\mathsf{dec}})$$
$$\text{return } m'.$$

[数192]

$$\mathsf{Delegate}_L(\mathsf{pk}, \mathsf{sk}_L, \vec{v}_{L+1} := (v_{L+1,1},\ldots,v_{L+1,n_{L+1}})):$$
$$\text{for } j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$$
$$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$$
$$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota),j},\ \sigma_{\mathsf{ran},(\tau,\iota)},$$
$$\phi_{\mathsf{ran},(\tau,\iota)},\ \alpha_{\mathsf{del},(\tau,\iota),j},\ \sigma_{\mathsf{del},(\tau,\iota)},\ \phi_{\mathsf{del},(\tau,\iota)},\ \psi',$$
$$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota),(t,i)} \xleftarrow{\mathsf{U}} \mathbb{R},$$

[数193]

$$
\begin{aligned}
k^*_{L+1,\mathrm{dec}} &:= k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L} \alpha_{\mathrm{dec},j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{dec}} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) + \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(t,i)} b^*_{t,n_t+u_t+i}, \\
k^*_{L+1,\mathrm{ran},j'} &:= \sum_{j=1}^{2L} \alpha_{\mathrm{ran},j',j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{ran},j'} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^*_{t,n_t+u_t+i}, \\
k^*_{L+1,\mathrm{ran},(\tau,\iota)} &:= \sum_{j=1}^{2L} \alpha_{\mathrm{ran},(\tau,\iota),j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{ran},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) \\
&\quad + \phi_{\mathrm{ran},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} \\
&\quad + \sum_{i=1}^{w_\tau} \eta_{\mathrm{ran},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}, \\
k^*_{L+1,\mathrm{del},(\tau,\iota)} &:= \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota),j}\, k^*_{L,\mathrm{ran},j} \\
&\quad + \sigma_{\mathrm{del},(\tau,\iota)} \Big(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}\Big) + \psi' k^*_{L,\mathrm{del},(\tau,\iota)} \\
&\quad + \phi_{\mathrm{del},(\tau,\iota)} k^*_{L,\mathrm{ran},(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} \\
&\quad + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} \\
&\quad + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}, \\
\mathsf{sk}_{L+1} &:= (k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)}, \\
&\qquad \{k^*_{L+1,\mathrm{ran},(\tau,\iota)}, k^*_{L+1,\mathrm{del},(\tau,\iota)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}), \\
&\text{return } \mathsf{sk}_{L+1}
\end{aligned}
$$

[0118] 実施の形態２で説明した階層的述語暗号方式を、環Ｒを係数とする加群において実現すると数１９４から数１９９のようになる。なお、Ｓｅｔｕｐアルゴリズムと$\mathsf{G}_{\circ b}$アルゴリズムとは、数１８６と数１８７とに示す通りであ

る。

[数194]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\rho_1),\ldots,(\vec{v}_L,\rho_L)) := (((v_{1,1},\ldots,v_{1,n_1})\in\mathbb{R}^{n_1},\rho_1\in\{0,1\}),\ldots,$$

$$((v_{L,1},\ldots,v_{L,n_L})\in\mathbb{R}^{n_L},\rho_L\in\{0,1\})):$$

$$\text{for } j=1,\ldots,2L;\ \tau=L+1,\ldots,d;\ (\tau,t)=(\tau,1),\ldots,(\tau,n_\tau);$$

$$\psi,s_{\mathsf{dec},t},s_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{R}\ (t=1,\ldots,L);$$

$$\theta_{\mathsf{dec},t},\theta_{\mathsf{ran},j,t}\xleftarrow{\mathsf{U}}\mathbb{R},$$

$$\vec{\eta}_{\mathsf{dec},t},\ \vec{\eta}_{\mathsf{ran},j,t},\ \vec{\eta}_{\mathsf{ran},0,t},\ \vec{\eta}_{\mathsf{del},0,t}\ \vec{\eta}_{\mathsf{del},1,t}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t}\ \ (t=0,\ldots,L);$$

$$s_{\mathsf{ran},0,t},s_{\mathsf{del},0,t},s_{\mathsf{del},1,t}\xleftarrow{\mathsf{U}}\mathbb{R},$$

$$\theta_{\mathsf{ran},0,t},\theta_{\mathsf{del},0,t},\theta_{\mathsf{del},1,t}\xleftarrow{\mathsf{U}}\mathbb{R},$$

$$\vec{\eta}_{\mathsf{ran},0,(\tau,t)},\ \vec{\eta}_{\mathsf{del},0,(\tau,t)},\ \vec{\eta}_{\mathsf{del},1,(\tau,t)}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t}\ ,(t=0,\ldots,L+1);$$

$$s_{\mathsf{dec},0}:=\sum_{t=1}^{L}s_{\mathsf{dec},t},\ s_{\mathsf{ran},j,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},j,t},\ s_{\mathsf{ran},0,0}:=\sum_{t=1}^{L}s_{\mathsf{ran},0,t},$$

$$s_{\mathsf{del},0,0}:=\sum_{t=1}^{L+1}s_{\mathsf{del},0,t},\ s_{\mathsf{del},1,0}:=\sum_{t=1}^{L+1}s_{\mathsf{del},1,t},$$

$$k^*_{L,\mathsf{dec}}:=(\ (-s_{\mathsf{dec},0},0^{u_0},1,\vec{\eta}_{\mathsf{dec},0},0^{z_0})_{\mathbb{B}^*_0},$$

$$\left\{\begin{array}{ll}(s_{\mathsf{dec},t}\vec{e}_{t,1}+\theta_{\mathsf{dec},t},\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathsf{dec},t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{dec},t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathsf{dec},t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$

$$:t=1,\ldots,L),$$

$$k^*_{L,\mathsf{ran},j}:=(\ (-s_{\mathsf{ran},j,0},0^{u_0},0,\vec{\eta}_{\mathsf{ran},j,0},0^{z_0})_{\mathbb{B}^*_0},$$

$$\left\{\begin{array}{ll}(s_{\mathsf{ran},j,t}\vec{e}_{t,1}+\theta_{\mathsf{ran},j,t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathsf{ran},j,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathsf{ran},j,t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathsf{ran},j,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$

$$:t=1,\ldots,L),$$

[数195]

$$k^*_{L,\mathsf{ran},(\tau,t,0)} := ((-s_{\mathsf{ran},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{ran},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{ran},0,t}\vec{e}_{t,1} + \theta_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{ran},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{ran},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{ran},0,L+1}\vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathsf{ran},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,0)} := ((-s_{\mathsf{del},0,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},0,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},0,t}\vec{e}_{t,1} + \theta_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{del},0,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},0,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{del},0,L+1}\vec{e}_{\tau,1}, +\psi\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},0,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$k^*_{L,\mathsf{del},(\tau,t,1)} := ((-s_{\mathsf{del},1,0}, 0^{u_0}, 0, \vec{\eta}_{\mathsf{del},1,0}, 0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{ \begin{array}{ll} (s_{\mathsf{del},1,t}\vec{e}_{t,1} + \theta_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 0 \\ (s_{\mathsf{del},1,t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathsf{del},1,t}, 0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t = 1 \end{array} \right\}$$
$$: t = 1, \ldots, L),$$
$$(s_{\mathsf{del},1,L+1}\vec{e}_{\tau,t}, 0^{u_\tau}, \vec{\eta}_{\mathsf{del},1,(\tau,t)}, 0^{z_\tau})_{\mathbb{B}^*_\tau}),$$

$$\mathsf{sk}_L := (((\vec{v}_1, \rho_1), \ldots, (\vec{v}_L, \rho_L));$$
$$k^*_{L,\mathsf{dec}}, \{k^*_{L,\mathsf{ran},j}\}_{j=1,\ldots,2L}, \{k^*_{L,\mathsf{ran},(\tau,t,0)}, k^*_{L,\mathsf{del},(\tau,t,0)}, k^*_{L,\mathsf{del},(\tau,t,1)}\}$$
$$\tau = L+1, \ldots, d; (\tau,t) = (\tau,1), \ldots, (\tau,n_\tau)),$$

return sk_L.

[数196]

$$\mathsf{Enc}(\mathsf{pk}, m \in \mathbb{G}_T, (\vec{x}_1,\ldots,\vec{x}_L) := ((x_{1,1},\ldots,x_{1,n_1}),\ldots,(x_{L,1},\ldots,x_{L,n_L})):$$

$$(\vec{x}_{L+1},\ldots,\vec{x}_d) \xleftarrow{\cup} \mathbb{R}^{n_{L+1}} \times \cdots \times \mathbb{R}^{n_d};$$

$$\omega, \zeta \xleftarrow{\cup} \mathbb{R},\ \vec{\varphi}_t \xleftarrow{\cup} \mathbb{R}^{z_t}\ (t = 0,\ldots,d),$$

$$c_1 := (\ (\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t}\ : t = 1,\ldots,d),$$

$$c_2 := g_T^{\zeta} m,$$

$$\mathsf{ct} := ((\vec{x}_1,\ldots,\vec{x}_L); c_1, c_2),$$

return ct.

[数197]

$$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_L, \mathsf{ct}):$$

$$K := e(c_{1,0}, k^*_{L,\mathsf{dec},0}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 0} e(c_{1,t}, k^*_{L,\mathsf{dec},t}) \cdot \prod_{1 \le t \le d \wedge \rho_t = 1} e(c_{1,t}, k^*_{L,\mathsf{dec},t})^{1/(\vec{v}_t \cdot \vec{x}_t)},$$

where $(k^*_{L,\mathsf{dec},0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, k^*_{L,\mathsf{dec},d} \in \langle \mathbb{B}^*_d \rangle) := k^*_{L,\mathsf{dec}}$,

$(c_{1,0} \in \langle \mathbb{B}^*_0 \rangle, \ldots, c_{1,d} \in \langle \mathbb{B}^*_d \rangle := c_1$,

$$m' := c_2 / K,$$

return m'.

[数198]

$$\mathsf{Delegate}_L(\mathsf{pk},\mathsf{sk}_L,(\vec{v}_{L+1},\rho_{L+1}):=((v_{L+1,1},\ldots,v_{L+1,n_{L+1}}),\rho_{L+1})):$$

for $j=1,\ldots,2L;\ j'=1,\ldots,2(L+1);\ \tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau);$

$t=0,\ldots,L+1,\tau;\ (t,i)=(t,1),\ldots,(t,w_t);$

$\alpha_{\mathsf{dec},j},\ \sigma_{\mathsf{dec}},\ \alpha_{\mathsf{ran},j',j},\ \sigma_{\mathsf{ran},j'},\ \alpha_{\mathsf{ran},(\tau,\iota,0),j},\ \sigma_{\mathsf{ran},(\tau,\iota,0)},\ \phi_{\mathsf{ran},(\tau,\iota,0)},$

$\alpha_{\mathsf{del},(\tau,\iota,0),j},\ \sigma_{\mathsf{del},(\tau,\iota,0)},\ \phi_{\mathsf{del},(\tau,\iota,0)},\ \alpha_{\mathsf{del},(\tau,\iota,1),j},\ \sigma_{\mathsf{del},(\tau,\iota,1)},\ \phi_{\mathsf{del},(\tau,\iota,1)},$

$\eta_{\mathsf{dec},(t,i)},\ \eta_{\mathsf{ran},j',(t,i)},\ \eta_{\mathsf{ran},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,0),(t,i)},\ \eta_{\mathsf{del},(\tau,\iota,1),(t,i)},$

$\psi_0,\psi_1,\xleftarrow{\cup}\mathbb{R},$

$$k^*_{L+1,\mathsf{dec}}:=k^*_{L,\mathsf{dec}}+\sum_{j=1}^{2L}\alpha_{\mathsf{dec},j}k^*_{L,\mathsf{ran},j}$$
$$+\left\{\begin{array}{ll}(\sigma_{\mathsf{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ (\sigma_{\mathsf{dec}}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(0,i)}b^*_{0,1+u_0+1+i}+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{dec},(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},j'}:=\sum_{j=1}^{2L}\alpha_{\mathsf{ran},j',j}k^*_{L,\mathsf{ran},j}$$
$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},j'}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ \sigma_{\mathsf{ran},j'}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(0,i)}b^*_{0,1+u_0+1+i}$$
$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{ran},j',(t,i)}b^*_{t,n_t+u_t+i},$$

$$k^*_{L+1,\mathsf{ran},(\tau,\iota,0)}:=\sum_{j=1}^{2L}\alpha_{\mathsf{ran},(\tau,\iota)j,}k^*_{L,\mathsf{ran},j}+\phi_{\mathsf{ran},(\tau,\iota,0)}k^*_{L,\mathsf{ran},(\tau,\iota,0)}$$
$$+\left\{\begin{array}{ll}\sigma_{\mathsf{ran},(\tau,\iota,0)}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathsf{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ \sigma_{\mathsf{ran},(\tau,\iota,0)}([k^*_{L,\mathsf{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathsf{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(0,i)}b^*_{0,1+u_0+1+i}$$
$$+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathsf{del},(\tau,\iota,0),(t,i)}b^*_{t,n_t+u_t+i}$$
$$+\sum_{i=1}^{w_\tau}\eta_{\mathsf{del},(\tau,\iota,0),(\tau,i)}b^*_{\tau,n_\tau+u_\tau+i},$$

[数199]

$$k^*_{L+1,\mathrm{del},(\tau,\iota,0)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^*_{L,\mathrm{ran}(\tau,\iota,0)}$$
$$+ \psi_0 k^*_{L,\mathrm{del}(\tau,\iota,0)}$$
$$+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,0)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$k^*_{L+1,\mathrm{del},(\tau,\iota,1)} := \sum_{j=1}^{2L} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^*_{L,\mathrm{ran},j} + \psi_1 k^*_{L,\mathrm{del}(\tau,\iota,1)}$$
$$+ \left\{ \begin{array}{ll} \sigma_{\mathrm{del},(\tau,\iota,1)} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} ([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t = 1 \end{array} \right\}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(0,i)} b^*_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^*_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$
$$\mathrm{sk}_{L+1} := (((\vec{v}_1,\rho_1),\ldots,(\vec{v}_{L+1},\rho_{L+1}));$$
$$k^*_{L+1,\mathrm{dec}}, \{k^*_{L+1,\mathrm{ran},j'}\}_{j'=1,\ldots,2(L+1)},$$
$$\{k^*_{L+1,\mathrm{ran},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,0)}, k^*_{L+1,\mathrm{del},(\tau,\iota,1)}\}_{\tau=L+2,\ldots,d;\ (\tau,\iota)=(\tau,1),\ldots,(\tau,n_\tau)}),$$
return sk_{L+1}.

[0119] 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、鍵委譲装置４００）のハードウェア構成について説明する。

図２０は、鍵生成装置１００、暗号化装置２００、復号装置３００、鍵委譲装置４００のハードウェア構成の一例を示す図である。

図２０に示すように、鍵生成装置１００、暗号化装置２００、復号装置３

００、鍵委譲装置４００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。

[0120] 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。

[0121] 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。

[0122] 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」、「マスター公開鍵取得部２１０」、「情報入力部２２０」、「暗号化データ生成部２３０」、「データ送信部２４０」、「復号鍵取得部３１０」、「データ受信部３２０」、「ペアリング演算部３３０」、「メッセージ計算部３４０」、「復号鍵取得部４１０」、「情報入力部４２０」、「委譲鍵生成部４３０」、「鍵配布部４４０」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「マスター公開鍵ｐｋ」、「マスター秘密鍵ｓｋ」、「復号鍵sk_L」、「委譲鍵sk_{L+1}」、「暗号化データｃｔ」、「属性情報」、「述語情報」、「メッセージｍ」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。

[0123] 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

[0124] １０　暗号処理システム、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　乱数生成部、１４２　復号要素生成部、１４３　ランダム化要素生成部、１４４　委譲要素生成部、１５０　鍵配布部、２００　暗号化装置、２１０　マスター公開鍵取得部、２２０　情報入力部、２２１　属性情報入力部、２２２　メッセージ入力部、２３０　暗号化データ生成部、２３１　乱数生成部、２３２　暗号化データｃ１生成部、２３３　暗号化データｃ２生成部、２４０　データ送信部、３００　復号装置、３１０　復号鍵取得部、３２０　データ受信部、３３０　ペアリング演算部、３４０　メッセージ計算部、４００　鍵委譲装置、４１０　復号鍵取得部、４２０　情報入力部、４３０　委譲鍵生成部、４３１　乱数生成部、４３２　下位復号要素生成部、４３３　下位ランダム化要素生成部、４３４　下位委譲要素生成部、４４０　鍵配布部。

請求の範囲

[請求項1] ｔ＝１，．．．．，Ｌ＋１（Ｌは１以上の整数）の各整数ｔについての基底$Ｂ_{t}$と基底$Ｂ^{*}_{t}$とを用いて暗号処理を行う暗号処理システムであり、

ｔ＝１，．．．．，Ｌのうち少なくとも一部の整数ｔについての基底$Ｂ_{t}$の基底ベクトルに属性情報$\vec{x}_{t}$を埋め込んだベクトルを暗号化データｃｔとして生成する暗号化装置と、

ｔ＝１，．．．．，Ｌの各整数ｔについての基底$Ｂ^{*}_{t}$の基底ベクトルに述語情報$\vec{v}_{t}$を埋め込んだベクトルを復号鍵$ｓｋ_{Ｌ}$として、前記暗号化装置が生成した暗号化データｃｔと前記復号鍵$ｓｋ_{Ｌ}$とについてペアリング演算を行い前記暗号化データｃｔを復号する復号装置と、

基底$Ｂ^{*}_{Ｌ＋１}$の基底ベクトルに述語情報$\vec{v}_{Ｌ＋１}$を埋め込んだベクトルと、前記復号装置が使用した復号鍵$ｓｋ_{Ｌ}$とに基づき、前記復号鍵$ｓｋ_{Ｌ}$の下位の復号鍵$ｓｋ_{Ｌ＋１}$を生成する鍵委譲装置と

を備えることを特徴とする暗号処理システム。

[請求項2] 前記暗号処理システムは、さらに、前記復号鍵$ｓｋ_{Ｌ}$を生成する鍵生成装置を備え、

前記鍵生成装置は、

ｔ＝１，．．．．，Ｌの各整数ｔについて述語情報$\vec{v}_{t}:=(v_{t,i})$（ｉ＝１，．．．．，$ｎ_{t}$）を入力する第１情報入力部と、

前記第１情報入力部が入力した述語情報$\vec{v}_{t}$と、所定の値Δと、ｔ＝１，．．．．，Ｌの各整数ｔについての所定の値$\theta_{dec,t}$と、$s_{dec,0}=\Sigma_{t=1}^{L}s_{dec,t}$であるようなｔ＝０，．．．．，Ｌの各整数ｔについての所定の値$s_{dec,t}$とを用いて、基底$Ｂ^{*}_{0}$の基底ベクトル$b^{*}_{0,p}$（ｐは所定の値）の係数として$-s_{dec,0}$を設定し、基底$Ｂ^{*}_{0}$の基底ベクトル$b^{*}_{0,q}$（ｑは所定の値）の係数として前記Δを設定し、ｔ＝１，．．．．，Ｌの各整数ｔについての基底$Ｂ^{*}_{t}$の基底ベクト

ルｂ*$_{t,i}$（ｉ＝１，．．．．，ｎ$_t$）の係数としてｓ$_{dec,t}$ｅ$^{\rightarrow}_{t,1}$＋θ$_{dec,t}$ｖ$_{t,i}$（ｉ＝１，．．．．，ｎ$_t$）を設定した復号要素ｋ*$_{L,dec}$を生成する復号要素生成部と、

前記復号要素生成部が生成した復号要素ｋ*$_{L,dec}$を含む復号鍵ｓｋ$_L$を前記復号装置へ送信する復号鍵送信部と

を備え、

前記暗号化装置は、

ｔ＝１，．．．．，Ｌの少なくとも一部の整数ｔについて属性情報ｘ$^{\rightarrow}_t$：＝（ｘ$_{t,i}$）（ｉ＝１，．．．．，ｎ$_t$）を入力する第２情報入力部と、

前記第２情報入力部が入力した属性情報ｘ$^{\rightarrow}_t$と、所定の値ω，ζとを用いて、基底Ｂ$_0$の基底ベクトルｂ$_{0,p}$の係数として前記ωを設定し、基底Ｂ$_0$の基底ベクトルｂ$_{0,q}$の係数として前記ζを設定し、前記少なくとも一部の整数ｔについての基底Ｂ$_t$の基底ベクトルｂ$_{t,i}$（ｉ＝１，．．．．，ｎ$_t$）の係数としてωｘ$_{t,i}$（ｉ＝１，．．．．，ｎ$_t$）を設定した暗号化データｃ$_1$を生成する暗号化データｃ１生成部と、

前記暗号化データｃ１生成部が生成した暗号化データｃ$_1$を含む暗号化データｃｔを前記復号装置へ送信するデータ送信部と

を備え、

前記復号装置は、

前記データ送信部が送信した暗号化データｃｔに含まれる暗号化データｃ$_1$と、前記復号鍵送信部が送信した前記復号鍵ｓｋ$_L$に含まれる復号要素ｋ*$_{L,dec}$とについて、ペアリング演算ｅ（ｃ$_1$，ｋ*$_{L,dec}$）を行うペアリング演算部

を備えることを特徴とする請求項１に記載の暗号処理システム。

［請求項3］ 前記暗号化装置は、さらに、

値ｇ$_T$＝ｅ（ｂ$_{0,1}$，ｂ*$_{0,1}$）と、前記Δと、前記ζとから得られ

る$g_T^{\Delta\zeta}$を、メッセージｍに乗じた暗号化データc_2を生成する暗号化データｃ２生成部

を備え、

前記データ送信部は、暗号化データc_1と、前記暗号化データｃ２生成部が生成した暗号化データc_2とを含む暗号化データｃｔを前記復号装置へ送信し、

前記ペアリング演算部は、前記ペアリング演算ｅ（c_1，$k^*_{L,dec}$）を行い、セッション鍵Ｋ：＝$g_T^{\Delta\zeta}$を計算し、

前記復号装置は、さらに、

前記ペアリング演算部が計算したセッション鍵Ｋで、前記暗号化データc_2を除して、前記メッセージｍを計算するメッセージ計算部

を備えることを特徴とする請求項２に記載の暗号処理システム。

［請求項4］ 前記鍵生成装置は、さらに、

$\tau=L+1$である整数τと、$\iota=1,\ldots,n_\tau$の各整数ιについて委譲要素$k^*_{L,del,(\tau,\iota)}$を生成する委譲要素生成部であって、$t=1,\ldots,L$の各整数ｔについての所定の値$\theta_{del,(\tau,\iota),t}$と、所定の値$\phi$と、$s_{del,(\tau,\iota),0}=\Sigma_{t=1}^{L+1}s_{del,(\tau,\iota),t}$であるような$t=0,\ldots,L+1$の各整数ｔについての所定の値$s_{del,(\tau,\iota),t}$とを用いて、基底$B^*_0$の基底ベクトル$b^*_{0,p}$の係数として$-s_{del,(\tau,\iota),0}$を設定し、$t=1,\ldots,L$の各整数ｔについての基底$B^*_t$の基底ベクトル$b^*_{t,i}$（$i=1,\ldots,n_t$）の係数として$s_{del,(\tau,\iota),t}\vec{e}_{t,1}+\theta_{del,(\tau,\iota),t}v_{t,i}$（$i=1,\ldots,n_t$）を設定し、基底$B^*_\tau$の基底ベクトル$b^*_{\tau,i}$（$i=1,\ldots,n_\tau$）の係数として$s_{del,(\tau,\iota),L+1}\vec{e}_{\tau,1}+\phi\vec{e}_{\tau,\iota}$（$i=1,\ldots,n_\tau$）を設定して委譲要素$k^*_{L,del,(\tau,\iota)}$を生成する委譲要素生成部

を備え、

前記復号鍵送信部は、前記復号要素$k^*_{L,dec}$と、前記委譲要素生

成部が生成した委譲要素$k^*_{L,del,(\tau,\iota)}$とを含む復号鍵sk_Lを前記委譲装置へ送信し、

前記鍵委譲装置は、

述語情報$\vec{v}_{L+1} := (v_{L+1,i})$ $(i=1,\ldots,n_{L+1})$を入力する第３情報入力部と、

前記第３情報入力部が入力した述語情報$\vec{v}_{L+1}$と、前記復号鍵送信部が送信した復号鍵sk_Lとを用いて、数１に示すベクトルを含む下位復号要素$k^*_{L+1,dec}$を生成する下位復号要素生成部と、

前記下位復号要素生成部が生成した下位復号要素$k^*_{L+1,dec}$を含む下位の復号鍵sk_{L+1}を下位の復号装置へ送信する委譲鍵送信部とを備えることを特徴とする請求項２に記載の暗号処理システム。

[数1]

$$k^*_{L,\mathrm{dec}} + \sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}$$

[請求項5] 前記暗号処理システムは、

少なくとも基底ベクトル$b_{0,i}$ $(i=1,\ldots,1+n_0,\ 1+n_0+1,\ldots,1+n_0+1+u_0,\ldots,1+n_0+1+u_0+w_0,\ldots,1+n_0+1+u_0+w_0+z_0)$ (n_0, u_0, w_0, z_0は１以上の整数）を有する基底B_0と、

少なくとも基底ベクトル$b^*_{0,i}$ $(i=1,\ldots,1+n_0,\ 1+n_0+1,\ldots,1+n_0+1+u_0,\ldots,1+n_0+1+u_0+w_0,\ldots,1+n_0+1+u_0+w_0+z_0)$ (n_0, u_0, w_0, z_0は１以上の整数）を有する基底B^*_0と、

少なくとも基底ベクトル$b_{t,i}$ $(i=1,\ldots,n_t,\ldots,n_t+u_t,\ldots,n_t+u_t+w_t,\ldots,n_t+u_t+w_t+z_t)$ (u_t, w_t, z_tは１以上の整数）を有する基底B_t $(t=1,\ldots,L+1)$と、

少なくとも基底ベクトル$b^*_{t,i}$ $(i=1,\ldots,n_t,\ldots,$

n_t+u_t，．．．，$n_t+u_t+w_t$，．．．，$n_t+u_t+w_t+z_t$）を有する基底B^*_t（$t=1,\ldots,L+1$）と

を用いて暗号処理を行い、

前記復号要素生成部は、$t=0,\ldots,L$の各整数tについての乱数$\vec{\eta}_{dec,t}:=(\eta_{dec,t,i})$（$i=1,\ldots,w_t$）に基づき、数２に示す復号要素を$k^*_{L,dec}$を生成し、

前記暗号化データｃ１生成部は、$t=0,\ldots,L$の各整数tについての乱数$\vec{\phi}_t:=(\phi_{t,i})$（$i=1,\ldots,z_t$）に基づき、数３に示す暗号化データ$c_1$を生成する

ことを特徴とする請求項２に記載の暗号処理システム。

[数2]

$$k^*_{L,\mathrm{dec}}:=\left(\ (-s_{\mathrm{dec},0},0^{u_0},\Delta,\vec{\eta}_{\mathrm{dec},0},0^{z_0})_{\mathbb{B}^*_0},\ (s_{\mathrm{dec},t}\,\vec{e}_{t,1}+\theta_{\mathrm{dec},t}\vec{v}_t,\ 0^{u_t},\vec{\eta}_{\mathrm{dec},t},0^{z_t})_{\mathbb{B}^*_t}:t=1,\ldots,L\right)$$

[数3]

$$c_1:=\left(\ (\omega,0^{u_0},\zeta,0^{w_0},\vec{\varphi}_0)_{\mathbb{B}_0},(\omega\vec{x}_t,0^{u_t},0^{w_t},\vec{\varphi}_t)_{\mathbb{B}t}:t=1,\ldots,L\right)$$

[請求項6] 前記鍵生成装置は、さらに、

$j=1,\ldots,2L$の各整数jについて、第１ランダム化要素$k^*_{L,ran,j}$を生成するとともに、$\tau=L+1,\ldots,d$（dは$L+1$以上の整数）の各整数τと、各整数τに関して$\iota=1,\ldots,n_\tau$の各整数ιとについて、第２ランダム化要素$k^*_{L,ran,(\tau,\iota)}$を生成するランダム化要素生成部であって、

$t=1,\ldots,L$の各整数tについての所定の値$\theta_{ran,j,t}$と、$s_{ran,j,0}=\Sigma_{t=1}{}^{L}s_{ran,j,t}$であるような$t=0,\ldots,L$についての所定の値$s_{ran,j,t}$と、$t=0,\ldots,L$の各整数$t$についての乱数$\vec{\eta}_{ran,j,t}:=(\eta_{ran,j,t,i})$（$i=1,\ldots,w_t$）とに基づき、数４に示す第１ランダム化要素$k^*_{L,ran,j}$を生成

し、

ｔ＝１，．．．，Ｌの各整数ｔについての所定の値$\theta_{ran,(\tau,\iota),t}$と、$s_{ran,(\tau,\iota),0}=\Sigma_{t=1}^{L+1}s_{ran,(\tau,\iota),t}$であるようなｔ＝０，．．．，Ｌ＋１についての所定の値$s_{ran,(\tau,\iota),t}$と、ｔ＝０，．．．，Ｌ＋１の各整数ｔについての乱数$\vec{\eta}_{ran,(\tau,\iota),t}:=(\eta_{ran,(\tau,\iota),t,i})$（ｉ＝１，．．．，$w_t$）とに基づき、数５に示す第２ランダム化要素$k^*_{L,ran,(\tau,\iota)}$を生成するランダム化要素生成部

を備え、

前記委譲要素生成部は、τ＝Ｌ＋１，．．．，ｄの各整数τと、各整数τに関してι＝１，．．．，n_τの各整数ιとについて、ｔ＝０，．．．，Ｌ＋１の各整数ｔについての乱数$\vec{\eta}_{del,(\tau,\iota),t}:=(\eta_{del,(\tau,\iota),t,i})$（ｉ＝１，．．．，$w_t$）に基づき、数６に示す委譲要素$k^*_{L,del,(\tau,\iota)}$を生成し、

前記復号鍵送信部は、前記復号要素$k^*_{L,dec}$と、前記ランダム化要素生成部が生成した第１ランダム化要素$k^*_{L,ran,j}$及び第２ランダム化要素$k^*_{L,ran,(\tau,\iota)}$と、前記委譲要素生成部が生成した委譲要素$k^*_{L,del,(\tau,\iota)}$とを含む復号鍵sk_Lを前記委譲装置へ送信し、

前記下位復号要素生成部は、前記述語情報$\vec{v}_{L+1}$と、前記復号鍵送信部が送信した復号鍵sk_Lと、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数$\alpha_{dec,j}$と、乱数σ_{dec}と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，w_tの各整数ｉとについての乱数$\eta_{dec,(t,i)}$とを用いて、数７に示す下位復号要素$k^*_{L+1,dec}$を生成する

ことを特徴とする請求項５に記載の暗号処理システム。

[数4]

$$k^*_{L,\mathrm{ran},j} := ((-s_{\mathrm{ran},j,0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},j,0}, 0^{z_0})_{\mathbb{B}^*_0}, (s_{\mathrm{ran},j,t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},j,t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},j,t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L)$$

[数5]

$$k^*_{L,\mathrm{ran},(\tau,\iota)} := ((-s_{\mathrm{ran},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{ran},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0}, (s_{\mathrm{ran},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{ran},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L (s_{\mathrm{ran},(\tau,\iota),L+1}\ \vec{e}_{\tau,1}, 0^{u_\tau}, \vec{\eta}_{\mathrm{ran},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

[数6]

$$k^*_{L,\mathrm{del},(\tau,\iota)} := ((-s_{\mathrm{del},(\tau,\iota),0}, 0^{u_0}, 0, \vec{\eta}_{\mathrm{del},(\tau,\iota),0}, 0^{z_0})_{\mathbb{B}^*_0}, (s_{\mathrm{del},(\tau,\iota),t}\ \vec{e}_{t,1} + \theta_{\mathrm{del},(\tau,\iota),t}\vec{v}_t,\ 0^{u_t}, \vec{\eta}_{\mathrm{del},(\tau,\iota),t}, 0^{z_t})_{\mathbb{B}^*_t} : t = 1,\ldots,L (s_{\mathrm{del},(\tau,\iota),L+1}\ \vec{e}_{\tau,1} + \psi\vec{e}_{\tau,\iota}, 0^{u_\tau}, \vec{\eta}_{\mathrm{del},(\tau,\iota),L+1}, 0^{z_\tau})_{\mathbb{B}^*_\tau})$$

[数7]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{j=1}^{2L+1} \alpha_{\mathrm{dec},j} k^*_{L,\mathrm{ran},j} + \sigma_{\mathrm{dec}} (\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i)}) + \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{dec},(t,i)} b^*_{t,n_t+u_t+i}$$

[請求項7] 前記委譲装置は、さらに、

ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’について、第１下位ランダム化要素ｋ*$_{Ｌ+1,\ ran,\ j'}$を生成するとともに、τ＝Ｌ＋２，．．．，ｄ（ｄはＬ＋２以上の整数）の各整数τと、各整数τに関してι＝１，．．．，ｎ$_τ$の各整数ιについて、第２下位ランダム化要素ｋ*$_{Ｌ+1,\ ran,\ (τ,\ ι)}$を生成

する下位ランダム化要素生成部であって、

前記述語情報$v^{\rightarrow}_{L+1}$と、前記復号鍵sk_Lと、j＝1，．．．，2Lの各整数jとj’＝1，．．．，2（L＋1）の各整数j’とについての乱数$\alpha_{ran,j',j}$と、j’＝1，．．．，2（L＋1）の各整数j’についての乱数$\sigma_{ran,j'}$と、t＝0，．．．，L＋1の各整数tとi＝1，．．．，w_tの各整数iとについての乱数$\eta_{ran,j',(t,i)}$とに基づき、数８に示す第１下位ランダム化要素$k^*_{L+1,ran,j'}$を生成し、

前記述語情報$v^{\rightarrow}_{L+1}$と、前記復号鍵sk_Lと、j＝1，．．．，2Lの各整数jについての乱数$\alpha_{ran,(\tau,\iota),j}$と、乱数$\sigma_{ran,(\tau,\iota)}$と、乱数$\phi_{ran,(\tau,\iota)}$と、t＝0，．．．，L＋1，$\tau$の各整数tとi＝1，．．．，$w_t$の各整数iとについての$\eta_{ran,(\tau,\iota),(t,i)}$とに基づき、数９に示す第２下位ランダム化要素$k^*_{L+1,ran,(\tau,\iota)}$を生成する下位ランダム化要素生成部と、

τ＝L＋2，．．．，d（dはL＋２以上の整数）の各整数τと、各整数τに関してι＝1，．．．，n_τの各整数ιについて、下位委譲要素$k^*_{L+1,del,(\tau,\iota)}$を生成する下位委譲要素生成部であって、前記述語情報$v^{\rightarrow}_{L+1}$と、前記復号鍵sk_Lと、j＝1，．．．，2Lの各整数jについての乱数$\alpha_{del,(\tau,\iota),j}$と、乱数$\sigma_{del,(\tau,\iota)}$と、乱数$\phi'$と、乱数$\phi_{del,(\tau,\iota)}$と、t＝0，．．．，L＋1，$\tau$の各整数tとi＝1，．．．，$w_t$の各整数iとについての$\eta_{del,(\tau,\iota),(t,i)}$とに基づき、数１０に示す下位委譲要素$k^*_{L+1,del,(\tau,\iota)}$を生成する下位委譲要素生成部と

を備え、

前記委譲鍵送信部は、前記下位復号要素生成部が生成した下位復号要素$k^*_{L+1,dec}$と、前記下位ランダム化要素生成部が生成した第１下位ランダム化要素$k^*_{L+1,ran,j'}$及び第２下位ランダム化要素$k^*_{L+1,ran,(\tau,\iota)}$と、前記下位委譲要素生成部が生成した下位委譲要

素$k^*_{L+1,del,(\tau,\iota)}$とを含む下位の復号鍵$sk_{L+1}$を下位の委譲装置へ送信する

ことを特徴とする請求項６に記載の暗号処理システム。

[数8]

$$k^*_{L+1,ran,j'} := \sum_{j=1}^{2L+1} \alpha_{ran,j',j} k^*_{L,ran,j} + \sigma_{ran,j'}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,del,(L+1,i)}\right) + \sum_{i=1}^{w_t} \eta_{ran,j',(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1}\sum_{i=1}^{w_t} \eta_{ran,j',(t,i)} b^*_{t,n_t+u_t+i}$$

[数9]

$$k^*_{L+1,ran,(\tau,\iota)} := \sum_{j=1}^{2L+1} \alpha_{ran,(\tau,\iota),j} k^*_{L,ran,j} + \sigma_{ran,(\tau,\iota)}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,del,(L+1,i)}\right) + \phi_{ran,(\tau,\iota)} k^*_{L,ran,(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{ran,(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1}\sum_{i=1}^{w_t} \eta_{ran,(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{ran,(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

[数10]

$$k^*_{L+1,del,(\tau,\iota)} := \sum_{j=1}^{2L+1} \alpha_{del,(\tau,\iota),j} k^*_{L,ran,j} + \sigma_{del,(\tau,\iota)}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,del,(L+1,i)}\right) + \psi' k^*_{L,del,(\tau,\iota)} + \phi_{del,(\tau,\iota)} k^*_{L,ran,(\tau,\iota)} + \sum_{i=1}^{w_t} \eta_{del,(\tau,\iota),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1}\sum_{i=1}^{w_t} \eta_{del,(\tau,\iota),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{del,(\tau,\iota),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i},$$

[請求項8] 前記第１情報入力部は、ｔ＝１，．．．，Ｌの各整数ｔについて述語情報（$\vec{v}_t := (v_{t,i})$ （ｉ＝１，．．．，n_t），$\rho_t \in \{0,1\}$）を入力し、

前記復号要素生成部は、基底ベクトル$b^*_{0,p}$の係数として$-s_{dec,0}$を設定し、基底ベクトル$b^*_{0,q}$の係数として前記Δを設定し、$t=1,\ldots,L$の各整数tについての基底ベクトル$b^*_{t,i}$の係数として、ρ_tが0の場合には$s_{dec,t}e^{\rightarrow}_{t,1}+\theta_{dec,t}v_{t,i}$（$i=1,\ldots,n_t$）を設定し、$\rho_t$が1の場合には$s_{dec,t}v_{t,i}$（$i=1,\ldots,n_t$）を設定した復号要素$k^*_{L,dec}$を生成することを特徴とする請求項2に記載の暗号処理システム。

[請求項9] 前記鍵生成装置は、さらに、

$\tau=L+1$である整数τと、$\iota=1,\ldots,n_\tau$の各整数ιについて第1委譲要素$k^*_{L,del,(\tau,\iota,0)}$と第2委譲要素$k^*_{L,del,(\tau,\iota,1)}$とを生成する委譲要素生成部であって、

$t=1,\ldots,L$の各整数tについての所定の値$\theta_{del,0,t}$と、所定の値ψと、$s_{del,0,0}=\Sigma_{t=1}^{L+1}s_{del,0,t}$であるような$t=0,\ldots,L+1$についての所定の値$s_{del,0,t}$とを用いて、基底$B^*_0$の基底ベクトル$b^*_{0,p}$の係数として$-s_{del,0,0}$を設定し、$t=1,\ldots,L$の各整数$t$についての基底$B^*_t$の基底ベクトル$b^*_{t,i}$（$i=1,\ldots,n_t$）の係数として、$\rho_t$が0の場合には$s_{del,0,t}e^{\rightarrow}_{t,1}+\theta_{del,0,t}v_{t,i}$（$i=1,\ldots,n_t$）を設定し、$\rho_t$が1の場合には$s_{del,0,t}v_{t,i}$（$i=1,\ldots,n_t$）を設定し、基底$B^*_\tau$の基底ベクトル$b^*_{\tau,i}$（$i=1,\ldots,n_\tau$）の係数として$s_{del,0,L+1}e^{\rightarrow}_{\tau,1}+\psi e^{\rightarrow}_{\tau,\iota}$（$i=1,\ldots,n_\tau$）を設定して第1委譲要素$k^*_{L,del,(\tau,\iota,0)}$を生成し、

$t=1,\ldots,L$の各整数tについての所定の値$\theta_{del,1,t}$と、$s_{del,1,0}=\Sigma_{t=1}^{L+1}s_{del,1,t}$であるような$t=0,\ldots,L+1$についての所定の値$s_{del,1,t}$とを用いて、基底$B^*_0$の基底ベクトル$b^*_{0,p}$の係数として$-s_{del,1,0}$を設定し、$t=1,\ldots,L$の各整数$t$についての基底$B^*_t$の基底ベクトル$b^*_{t,i}$（$i=1$

，．．．．，n_t）の係数として、ρ_tが０の場合には$s_{del,1,t}\vec{e}_{t,1}+\theta_{del,1,t}v_{t,i}$（ｉ＝１，．．．，$n_t$）を設定し、$\rho_t$が１の場合には$s_{del,1,t}v_{t,i}$（ｉ＝１，．．．，$n_t$）を設定し、基底Ｂ$^*_\tau$の基底ベクトル$b^*_{\tau,i}$（ｉ＝１，．．．，$n_\tau$）の係数として$s_{del,1,L+1}\vec{e}_{\tau,1}$（ｉ＝１，．．．，$n_\tau$）を設定して第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$を生成する委譲要素生成部

を備え、

前記復号鍵送信部は、前記復号要素$k^*_{L,dec}$と、前記委譲要素生成部が生成した第１委譲要素$k^*_{L,del,(\tau,\iota,0)}$及び第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$とを含む復号鍵$sk_L$を前記委譲装置へ送信し、

前記鍵委譲装置は、

述語情報（$\vec{v}_{L+1}$：＝（$v_{L+1,i}$）（ｉ＝１，．．．，n_{L+1}），$\rho_{L+1}\in\{0,1\}$）を入力する第３情報入力部と、

前記第３情報入力部が入力した述語情報$\vec{v}_{L+1}$と、前記復号鍵送信部が送信した復号鍵sk_Lとを用いて、数１１に示すベクトルを含む下位復号要素$k^*_{L+1,dec}$を生成する下位復号要素生成部

を備えることを特徴とする請求項８に記載の暗号処理システム。

[数11]

$$k^*_{L,\mathrm{dec}}+\left\{\begin{array}{ll}(\sigma_{\mathrm{dec}}(\sum_{t=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ (\sigma_{\mathrm{dec}}([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$

[請求項10] 前記暗号処理システムは、

少なくとも基底ベクトル$b_{0,i}$（ｉ＝１，．．．，１＋n_0，１＋n_0＋１，．．．，１＋n_0＋１＋u_0，．．．，１＋n_0＋１＋u_0＋w_0，．．．，１＋n_0＋１＋u_0＋w_0＋z_0）（n_0，u_0，w_0，z_0は１以上の整数）を有する基底Ｂ$_0$と、

少なくとも基底ベクトル$b^*_{0,i}$（ｉ＝１，．．．，１＋n_0，１＋

$n_0+1, \ldots, 1+n_0+1+u_0, \ldots, 1+n_0+1+u_0+w_0, \ldots, 1+n_0+1+u_0+w_0+z_0$）（$n_0$，$u_0$，$w_0$，$z_0$は１以上の整数）を有する基底$B^*_0$と、

少なくとも基底ベクトル$b_{t,i}$（$i=1, \ldots, n_t, \ldots, n_t+u_t, \ldots, n_t+u_t+w_t, \ldots, n_t+u_t+w_t+z_t$）（$u_t$，$w_t$，$z_t$は１以上の整数）を有する基底$B_t$（$t=1, \ldots, L+1$）と、

少なくとも基底ベクトル$b^*_{t,i}$（$i=1, \ldots, n_t, \ldots, n_t+u_t, \ldots, n_t+u_t+w_t, \ldots, n_t+u_t+w_t+z_t$）を有する基底$B^*_t$（$t=1, \ldots, L+1$）と

を用いて暗号処理を行い、

前記復号要素生成部は、$t=0, \ldots, L$の各整数tについての乱数$\vec{\eta}_{dec,t} := (\eta_{dec,t,i})$（$i=1, \ldots, w_t$）に基づき、数１２に示す復号要素を$k^*_{L,dec}$を生成し、

前記暗号化データｃ１生成部は、$t=0, \ldots, L$の各整数tについての乱数$\vec{\phi}_t := (\phi_{t,i})$（$i=1, \ldots, z_t$）に基づき、数１３に示す暗号化データ$c_1$を生成する

ことを特徴とする請求項８に記載の暗号処理システム。

[数12]

$$k^*_{L,\mathrm{dec}} := \Big((-s_{\mathrm{dec},0}, 0^{u_0}, 1, \vec{\eta}_{\mathrm{dec},0}, 0^{z_0})_{\mathbb{B}^*_0}, \left\{ \begin{array}{ll} (s_{\mathrm{dec},t}\vec{e}_{t,1} + \theta_{\mathrm{dec},t}, \vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \mathrm{if}\ \rho_t = 0 \\ (s_{\mathrm{dec},t}\vec{v}_t, 0^{u_t}, \vec{\eta}_{\mathrm{dec},t}, 0^{z_t})_{\mathbb{B}^*_t}, & \mathrm{if}\ \rho_t = 1 \end{array} \right\} : t = 1, \ldots, L \Big)$$

[数13]

$$c_1 := \Big((\omega, 0^{u_0}, \zeta, 0^{w_0}, \vec{\varphi}_0)_{\mathbb{B}_0}, (\omega\vec{x}_t, 0^{u_t}, 0^{w_t}, \vec{\varphi}_t)_{\mathbb{B}t} : t = 1, \ldots, L \Big)$$

［請求項11］ 前記鍵生成装置は、さらに、

ｊ＝１，．．．，２Ｌの各整数ｊについて、第１ランダム化要素ｋ$^{*}_{L,ran,j}$を生成するとともに、τ＝Ｌ＋１，．．．，ｄ（ｄはＬ＋１以上の整数）の各整数τと、各整数τに関してι＝１，．．．，n_{τ}の各整数ιとについて、第２ランダム化要素ｋ$^{*}_{L,ran,(\tau,\iota,0)}$を生成するランダム化要素生成部であって、

ｔ＝１，．．．，Ｌの各整数ｔについての所定の値$\theta_{ran,j,t}$と、$s_{ran,j,0}=\Sigma_{t=1}^{L}s_{ran,j,t}$であるようなｔ＝０，．．．，Ｌについての所定の値$s_{ran,j,t}$と、ｔ＝０，．．．，Ｌの各整数ｔについての乱数$\vec{\eta}_{ran,j,t}:=(\eta_{ran,j,t,i})$（ｉ＝１，．．．，$w_t$）に基づき、数１４に示す第１ランダム化要素ｋ$^{*}_{L,ran,j}$を生成し、

ｔ＝１，．．．，Ｌの各整数ｔについての所定の値$\theta_{ran,0,t}$と、$s_{ran,0,0}=\Sigma_{t=1}^{L+1}s_{ran,0,t}$であるようなｔ＝０，．．．，Ｌ＋１についての所定の値$s_{ran,0,t}$と、ｔ＝０，．．．，Ｌの各整数ｔについての乱数$\vec{\eta}_{ran,0,t}:=(\eta_{ran,0,t,i})$（ｉ＝１，．．．，$w_t$）と、乱数$\vec{\eta}_{ran,0,(\tau,\iota)}:=(\eta_{ran,0,(\tau,\iota),i})$（ｉ＝１，．．．，$w_t$）とに基づき、数１５に示す第２ランダム化要素ｋ$^{*}_{L,ran,(\tau,\iota,0)}$を生成するランダム化要素生成部

を備え、

前記委譲要素生成部は、τ＝Ｌ＋１，．．．，ｄの各整数τと、各整数τに関してι＝１，．．．，n_{τ}の各整数ιとについて、ｔ＝０，．．．，Ｌの各整数ｔについての乱数$\vec{\eta}_{del,0,t}:=(\eta_{del,0,t,i})$（ｉ＝１，．．．，$w_t$）と、乱数$\vec{\eta}_{del,0,(\tau,\iota)}:=(\eta_{del,0,(\tau,\iota),i})$（ｉ＝１，．．．，$w_t$）とに基づき、数１６に示す第１委譲要素ｋ$^{*}_{L,del,(\tau,\iota,0)}$を生成するとともに、$\tau$＝Ｌ＋１，．．．，ｄの各整数$\tau$と、各整数$\tau$に関して$\iota$＝１，．．．，$n_{\tau}$の各整数$\iota$とについて、ｔ＝０，．．．，Ｌの各整数ｔについて

の乱数$\vec{\eta}_{del,1,t}:=(\eta_{del,1,t,i})$（ｉ＝１，．．．，$w_t$）と、乱数$\vec{\eta}_{del,1,(\tau,\iota)}:=(\eta_{del,1,(\tau,\iota),i})$（ｉ＝１，．．．，$w_t$）とに基づき

、数１７に示す第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$を生成し、

前記復号鍵送信部は、前記復号要素$k^*_{L,dec}$と、前記ランダム化要素生成部が生成した第１ランダム化要素$k^*_{L,ran,j}$及び第２ランダム化要素$k^*_{L,ran,(\tau,\iota,0)}$と、前記委譲要素生成部が生成した第１委譲要素$k^*_{L,del,(\tau,\iota,0)}$及び第２委譲要素$k^*_{L,del,(\tau,\iota,1)}$とを含む復号鍵$sk_L$を前記委譲装置へ送信し、

前記下位復号要素生成部は、前記述語情報$\vec{v}_{L+1}$と、前記復号鍵送信部が送信した復号鍵sk_Lと、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数$\alpha_{dec,j}$と、乱数σ_{dec}と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，w_tの各整数ｉとについての乱数$\eta_{dec,(t,i)}$とを用いて、数１８に示す下位復号要素$k^*_{L+1,dec}$を生成する

ことを特徴とする請求項１０に記載の暗号処理システム。

[数14]

$$k^*_{L,\mathrm{ran},j}:=\Big(\ (-s_{\mathrm{ran},j,0},0^{u_0},0,\vec{\eta}_{\mathrm{ran},j,0},0^{z_0})_{\mathbb{B}^*_0},\ \left\{\begin{array}{ll}(s_{\mathrm{ran},j,t}\vec{e}_{t,1}+\theta_{\mathrm{ran},j,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathrm{ran},j,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathrm{ran},j,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathrm{ran},j,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}\ :t=1,\ldots,L\Big)$$

[数15]

$$k^*_{L,\mathrm{ran},(\tau,t,0)}:=\Big(\ (-s_{\mathrm{ran},0,0},0^{u_0},0,\vec{\eta}_{\mathrm{ran},0,0},0^{z_0})_{\mathbb{B}^*_0},\ \left\{\begin{array}{ll}(s_{\mathrm{ran},0,t}\vec{e}_{t,1}+\theta_{\mathrm{ran},0,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathrm{ran},0,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathrm{ran},0,t}\vec{v}_t,0^{u_t},\vec{\eta}_{\mathrm{ran},0,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}\ :t=1,\ldots,L),\ (s_{\mathrm{ran},0,L+1}\vec{e}_{\tau,1},0^{u_\tau},\vec{\eta}_{\mathrm{ran},0,(\tau,t)},0^{z_\tau})_{\mathbb{B}^*_\tau}\Big)$$

[数16]

$$k^*_{L,\mathrm{del},(\tau,\iota,0)} := (\ (-s_{\mathrm{del},0,0},0^{u_0},0,\vec{\eta}_{\mathrm{del},0,0},0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathrm{del},0,t}\vec{e}_{t,1}+\theta_{\mathrm{del},0,t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathrm{del},0,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathrm{del},0,t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathrm{del},0,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$
$$:t=1,\ldots,L),$$
$$(s_{\mathrm{del},0,L+1}\vec{e}_{\tau,1},+\psi\vec{e}_{\tau,\iota},0^{u_\tau},\ \vec{\eta}_{\mathrm{del},0,(\tau,\iota)},0^{z_\tau})_{\mathbb{B}^*_\tau})$$

[数17]

$$k^*_{L,\mathrm{del},(\tau,\iota,1)} := (\ (-s_{\mathrm{del},1,0},0^{u_0},0,\vec{\eta}_{\mathrm{del},1,0},0^{z_0})_{\mathbb{B}^*_0},$$
$$\left\{\begin{array}{ll}(s_{\mathrm{del},1,t}\vec{e}_{t,1}+\theta_{\mathrm{del},1,t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathrm{del},1,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=0\\ (s_{\mathrm{del},1,t}\vec{v}_t,0^{u_t},\ \vec{\eta}_{\mathrm{del},1,t},0^{z_t})_{\mathbb{B}^*_t}, & \text{if } \rho_t=1\end{array}\right\}$$
$$:t=1,\ldots,L),$$
$$(s_{\mathrm{del},1,L+1}\vec{e}_{\tau,\iota},0^{u_\tau},\ \vec{\eta}_{\mathrm{del},1,(\tau,\iota)},0^{z_\tau})_{\mathbb{B}^*_\tau})$$

[数18]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}}+\sum_{j=1}^{2L+1}\alpha_{\mathrm{dec},j}k^*_{L,\mathrm{ran},j}$$
$$+\left\{\begin{array}{ll}(\sigma_{\mathrm{dec}}(\sum_{i=1}^{n_{L+1}}v_{L+1,i}k^*_{L,\mathrm{del},(L+1,i,0)}) & \text{if } \rho_t=0\\ (\sigma_{\mathrm{dec}}([k^*_{L,\mathrm{del},(L+1,i,1)}]^L & \\ \quad+\sum_{i=1}^{n_{L+1}}v_{L+1,i}[k^*_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}}) & \text{if } \rho_t=1\end{array}\right\}$$
$$+\sum_{i=1}^{w_t}\eta_{\mathrm{dec},(0,i)}b^*_{0,1+u_0+1+i}+\sum_{t=1}^{L+1}\sum_{i=1}^{w_t}\eta_{\mathrm{dec},(t,i)}b^*_{t,n_t+u_t+i}$$

[請求項12] 前記委譲装置は、さらに、

ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’について、第１下位ランダム化要素ｋ*$_{Ｌ+1,\ ran,\ j'}$を生成するとともに、τ＝Ｌ＋２，．．．，ｄ（ｄはＬ＋２以上の整数）の各整数τと、各整数τに関してι＝１，．．．，ｎ$_{\tau}$の各整数ιについて、第２下位ランダム化要素ｋ*$_{Ｌ+1,\ ran,\ (\tau,\ \iota,\ 0)}$を生成する下位ランダム化要素生成部であ

って、

前記述語情報$\vec{v}_{L+1}$と、前記復号鍵sk_Lと、ｊ＝１，．．．，２Ｌの各整数ｊとｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’とについての乱数$\alpha_{ran,j',j}$と、ｊ’＝１，．．．，２（Ｌ＋１）の各整数ｊ’についての乱数$\sigma_{ran,j'}$と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，w_tの各整数ｉとについての乱数$\eta_{ran,j',(t,i)}$とに基づき、数１９に示す第１下位ランダム化要素$k^*_{L+1,ran,j'}$を生成し、

前記述語情報$\vec{v}_{L+1}$と、前記復号鍵sk_Lと、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数$\alpha_{ran,(\tau,\iota),j}$と、乱数$\sigma_{ran,(\tau,\iota,0)}$と、乱数$\phi_{ran,(\tau,\iota,0)}$と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，w_tの各整数ｉとについての$\eta_{ran,(\tau,\iota,0),(t,i)}$とに基づき、数２０に示す第２下位ランダム化要素$k^*_{L+1,ran,(\tau,\iota,0)}$を生成する下位ランダム化要素生成部と、

τ＝Ｌ＋２，．．．，ｄ（ｄはＬ＋２以上の整数）の各整数τと、各整数τに関してι＝１，．．．，n_τの各整数ιについて、第１下位委譲要素$k^*_{L+1,del,(\tau,\iota,0)}$と第２下位委譲要素$k^*_{L+1,del,(\tau,\iota,1)}$とを生成する下位委譲要素生成部であって、

前記述語情報$\vec{v}_{L+1}$と、前記復号鍵sk_Lと、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数$\alpha_{del,(\tau,\iota,0),j}$と、乱数$\sigma_{del,(\tau,\iota,0)}$と、乱数$\phi_0$と、乱数$\phi_{del,(\tau,\iota,0)}$と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，w_tの各整数ｉとについての$\eta_{del,(\tau,\iota,0),(t,i)}$とに基づき、数２１に示す第１下位委譲要素$k^*_{L+1,del,(\tau,\iota,0)}$を生成し、

前記述語情報$\vec{v}_{L+1}$と、前記復号鍵sk_Lと、ｊ＝１，．．．，２Ｌの各整数ｊについての乱数$\alpha_{del,(\tau,\iota,1),j}$と、乱数$\sigma_{del,(\tau,\iota,1)}$と、乱数$\phi_1$と、乱数$\phi_{del,(\tau,\iota,1)}$と、ｔ＝０，．．．，Ｌ＋１の各整数ｔとｉ＝１，．．．，w_tの各整数ｉとについてのη_{de}

l，（τ，ι，1），（t，i）とに基づき、数２２に示す第２下位委譲要素ｋ＊Ｌ＋１，ｄｅｌ，（τ，ι，１）を生成する下位委譲要素生成部と

を備える

ことを特徴とする請求項１１に記載の暗号処理システム。

[数19]

$$k^*_{L+1,\mathrm{ran},j'} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},j',j} k^*_{L,\mathrm{ran},j} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},j'}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}\right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{ran},j'}\left([k^*_{L,\mathrm{del},(L+1,i,1)}]^L \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_L\right) & \text{if } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{ran},j',(t,i)} b^*_{t,n_t+u_t+i}$$

[数20]

$$k^*_{L+1,\mathrm{ran}(\tau,\iota,0)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{ran},(\tau,\iota)j,} k^*_{L,\mathrm{ran},j} + \phi_{\mathrm{ran},(\tau,\iota,0)} k^*_{L,\mathrm{ran},(\tau,\iota,0)} + \left\{ \begin{array}{ll} \sigma_{\mathrm{ran},(\tau,\iota,0)}\left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^*_{L,\mathrm{del},(L+1,i,0)}\right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{ran},(\tau,\iota,0)}\left([k^*_{L,\mathrm{del},(L+1,i,1)}]^L \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^*_{L,\mathrm{del},(L+1,i,1)}]_L\right) & \text{if } \rho_t = 1 \end{array} \right\} + \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^*_{0,1+u_0+1+i} + \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^*_{t,n_t+u_t+i} + \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^*_{\tau,n_\tau+u_\tau+i}$$

[数21]

$$k^{*}_{L+1,\mathrm{del}(\tau,\iota,0)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{del},(\tau,\iota,0),j} k^{*}_{L,\mathrm{ran},j} + \phi_{\mathrm{del},(\tau,\iota,0)} k^{*}_{L,\mathrm{ran}(\tau,\iota,0)}$$
$$+ \psi_0 k^{*}_{L,\mathrm{del}(\tau,\iota,0)}$$
$$+ \begin{cases} \sigma_{\mathrm{del},(\tau,\iota,0)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,0)} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{if } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(0,i)} b^{*}_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,0),(t,i)} b^{*}_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,0),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

[数22]

$$k^{*}_{L+1,\mathrm{del}(\tau,\iota,1)} := \sum_{j=1}^{2L+1} \alpha_{\mathrm{del}(\tau,\iota,1),j} k^{*}_{L,\mathrm{ran},j} + \psi_1 k^{*}_{L,\mathrm{del}(\tau,\iota,1)}$$
$$+ \begin{cases} \sigma_{\mathrm{del},(\tau,\iota,1)} \left(\sum_{i=1}^{n_{L+1}} v_{L+1,i} k^{*}_{L,\mathrm{del},(L+1,i,0)} \right) & \text{if } \rho_t = 0 \\ \sigma_{\mathrm{del},(\tau,\iota,1)} \left([k^{*}_{L,\mathrm{del},(L+1,i,1)}]^{L} \right. & \\ \qquad \left. + \sum_{i=1}^{n_{L+1}} v_{L+1,i} [k^{*}_{L,\mathrm{del},(L+1,i,1)}]_{\mathrm{L}} \right) & \text{if } \rho_t = 1 \end{cases}$$
$$+ \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(0,i)} b^{*}_{0,1+u_0+1+i}$$
$$+ \sum_{t=1}^{L+1} \sum_{i=1}^{w_t} \eta_{\mathrm{del},(\tau,\iota,1),(t,i)} b^{*}_{t,n_t+u_t+i}$$
$$+ \sum_{i=1}^{w_\tau} \eta_{\mathrm{del},(\tau,\iota,1),(\tau,i)} b^{*}_{\tau,n_\tau+u_\tau+i}$$

[請求項13] ｔ＝１，．．．．，Ｌ（Ｌは１以上の整数）の各整数ｔについての基底Ｂ$_t$と基底Ｂ$^*{}_t$とを用いて暗号処理を行う暗号処理システムにおいて、復号鍵ｓｋ$_L$を生成する鍵生成装置であり、

ｔ＝１，．．．．，Ｌの各整数ｔについて述語情報ｖ$^{\rightarrow}{}_t$：＝（ｖ$_{t,i}$）（ｉ＝１，．．．．，ｎ$_t$）を入力する第１情報入力部と、

前記第１情報入力部が入力した述語情報ｖ$^{\rightarrow}{}_t$と、所定の値Δと、ｔ＝１，．．．．，Ｌの各整数ｔについての所定の値$\theta_{dec,t}$と、ｓ$_{de}$

$_{c,0}=\Sigma_{t=1}{}^{L}s_{dec,t}$であるようなｔ＝０，．．．，Ｌの各整数ｔについての所定の値$s_{dec,t}$とを用いて、基底B^*_0の基底ベクトル$b^*_{0,p}$（ｐは所定の値）の係数として$-s_{dec,0}$を
設定し、基底B^*_0の基底ベクトル$b^*_{0,q}$（ｑは所定の値）の係数として前記Δを設定し、ｔ＝１，．．．，Ｌの各整数ｔについての基底B^*_tの基底ベクトル$b^*_{t,i}$（ｉ＝１，．．．，n_t）の係数として$s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$（ｉ＝１，．．．，$n_t$）を設定した復号要素$k^*_{L,dec}$を生成する復号要素生成部と、

前記復号要素生成部が生成した復号要素$k^*_{L,dec}$を含む復号鍵sk_Lを復号装置へ送信する復号鍵送信部と
を備えることを特徴とする鍵生成装置。

［請求項14］ ｔ＝１，．．．，Ｌ（Ｌは１以上の整数）の各整数ｔについての基底B_tと基底B^*_tとを用いて暗号処理を行う暗号処理システムにおいて、暗号化データｃｔを生成する暗号化装置であり、

ｔ＝１，．．．，Ｌの少なくとも一部の整数ｔについて属性情報$\vec{x}_t:=(x_{t,i})$（ｉ＝１，．．．，n_t）を入力する第２情報入力部と、

前記第２情報入力部が入力した属性情報$\vec{x}_t$と、所定の値ω，ζとを用いて、基底B_0の基底ベクトル$b_{0,p}$（ｐは所定の値）の係数として前記ωを設定し、基底B_0の基底ベクトル$b_{0,q}$（ｑは所定の値）の係数として前記ζを設定し、前記少なくとも一部の整数ｔについての基底B_tの基底ベクトル$b_{t,i}$（ｉ＝１，．．．，n_t）の係数として$\omega x_{t,i}$（ｉ＝１，．．．，n_t）を設定した暗号化データc_1を生成する暗号化データｃ１生成部と、

前記暗号化データｃ１生成部が生成した暗号化データc_1を含む暗号化データｃｔを復号装置へ送信するデータ送信部と
を備えることを特徴とする暗号化装置。

［請求項15］ ｔ＝１，．．．，Ｌ（Ｌは１以上の整数）の各整数ｔについての基

底B_tと基底B^*_tとを用いて暗号処理を行う暗号処理システムにおいて、暗号化データc_1を復号鍵sk_Lにより復号する復号装置であり、

属性情報$\vec{x}_t := (x_{t,i})$（$i=1,\ldots,n_t$）と、所定の値ω，ζとを用いて、基底B_0の基底ベクトル$b_{0,p}$（pは所定の値）の係数として前記ωを設定し、基底B_0の基底ベクトル$b_{0,q}$（qは所定の値）の係数として前記ζを設定し、前記少なくとも一部の整数tについての基底B_tの基底ベクトル$b_{t,i}$（$i=1,\ldots,n_t$）の係数として$\omega x_{t,i}$（$i=1,\ldots,n_t$）を設定した暗号化データc_1を暗号化装置から受信するデータ受信部と、

述語情報$\vec{v}_t := (v_{t,i})$（$i=1,\ldots,n_t$）と、所定の値Δと、$t=1,\ldots,L$の各整数tについての所定の値$\theta_{dec,t}$と、$s_{dec,0}=\Sigma_{t=1}^{L} s_{dec,t}$であるような$t=0,\ldots,L$の各整数$t$についての所定の値$s_{dec,t}$とを用いて、基底$B^*_0$の基底ベクトル$b^*_{0,p}$（$p$は所定の値）の係数として$-s_{dec,0}$を設定し、基底$B^*_0$の基底ベクトル$b^*_{0,q}$（$q$は所定の値）の係数として前記$\Delta$を設定し、$t=1,\ldots,L$の各整数$t$についての基底$B^*_t$の基底ベクトル$b^*_{t,i}$（$i=1,\ldots,n_t$）の係数として$s_{dec,t}\vec{e}_{t,1}+\theta_{dec,t}v_{t,i}$（$i=1,\ldots,n_t$）を設定した復号要素$k^*_{L,dec}$を含む復号鍵$sk_L$を鍵生成装置から取得する復号鍵取得部と、

前記データ受信部が受信した暗号化データc_1と、前記復号鍵取得部が取得した前記復号鍵sk_Lに含まれる復号要素$k^*_{L,dec}$とについて、ペアリング演算$e(c_1, k^*_{L,dec})$を行い、前記暗号化データc_1を復号するペアリング演算部と

を備えることを特徴とする復号装置。

［請求項16］ $t=1,\ldots,L+1$（Lは1以上の整数）の各整数tについての基底B_tと基底B^*_tとを用いて暗号処理を行う暗号処理システムに

おいて、復号鍵sk_Lの下位の復号鍵sk_{L+1}を生成する鍵委譲装置であり、

$t=1,\ldots,L$の各整数tについての基底B^*_tの基底ベクトルに述語情報$\vec{v}_t$を埋め込んだベクトルを復号鍵sk_Lとして取得する復号鍵取得部と、

前記復号鍵取得部が取得した復号鍵sk_Lと、基底B^*_{L+1}の基底ベクトルに述語情報$\vec{v}_{L+1}$を埋め込んだベクトルとに基づき、前記復号鍵sk_Lの下位の復号鍵sk_{L+1}を生成する委譲鍵生成部と

を備えることを特徴とする鍵委譲装置。

[請求項17] $t=1,\ldots,L+1$（Lは1以上の整数）の各整数tについての基底B_tと基底B^*_tとを用いた暗号処理方法であり、

暗号化装置が、$t=1,\ldots,L$のうち少なくとも一部の整数tについての基底B_tの基底ベクトルに属性情報$\vec{x}_t$を埋め込んだベクトルを暗号化データctとして生成する暗号化工程と、

復号装置が、$t=1,\ldots,L$の各整数tについての基底B^*_tの基底ベクトルに述語情報$\vec{v}_t$を埋め込んだベクトルを復号鍵sk_Lとして、前記暗号化工程で生成した暗号化データctと前記復号鍵sk_Lとについて、ペアリング演算を行い前記暗号化データctを復号する復号工程と、

鍵委譲装置が、基底B^*_{L+1}の基底ベクトルに述語情報を埋め込んだベクトル$\vec{v}_{L+1}$と、前記復号工程で使用した復号鍵sk_Lとに基づき、前記復号鍵sk_Lの下位の復号鍵sk_{L+1}を生成する鍵委譲工程と

を備えることを特徴とする暗号処理方法。

[請求項18] $t=1,\ldots,L+1$（Lは1以上の整数）の各整数tについての基底B_tと基底B^*_tとを用いて暗号処理を実行する暗号処理プログラムであり、

$t=1,\ldots,L$のうち少なくとも一部の整数tについての基底

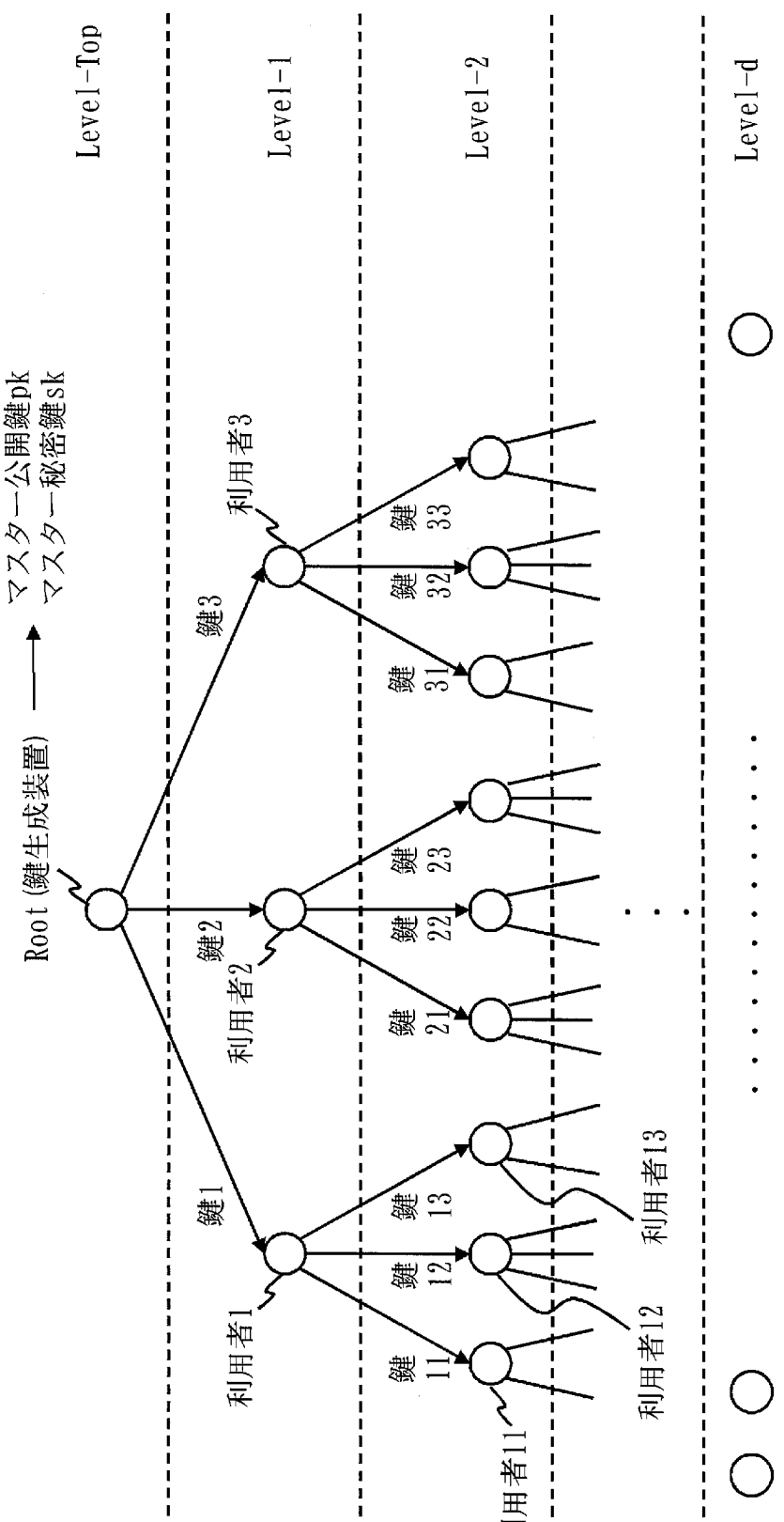
B_tの基底ベクトルに属性情報$\vec{x}_t$を埋め込んだベクトルを暗号化データｃｔとして生成する暗号化処理と、

ｔ＝１，．．．，Ｌの各整数ｔについての基底B^*_tの基底ベクトルに述語情報$\vec{v}_t$を埋め込んだベクトルを復号鍵sk_Lとして、前記暗号化装置が生成した暗号化データｃｔと前記復号鍵sk_Lとについて、ペアリング演算を行い前記暗号化データｃｔを復号する復号処理と、

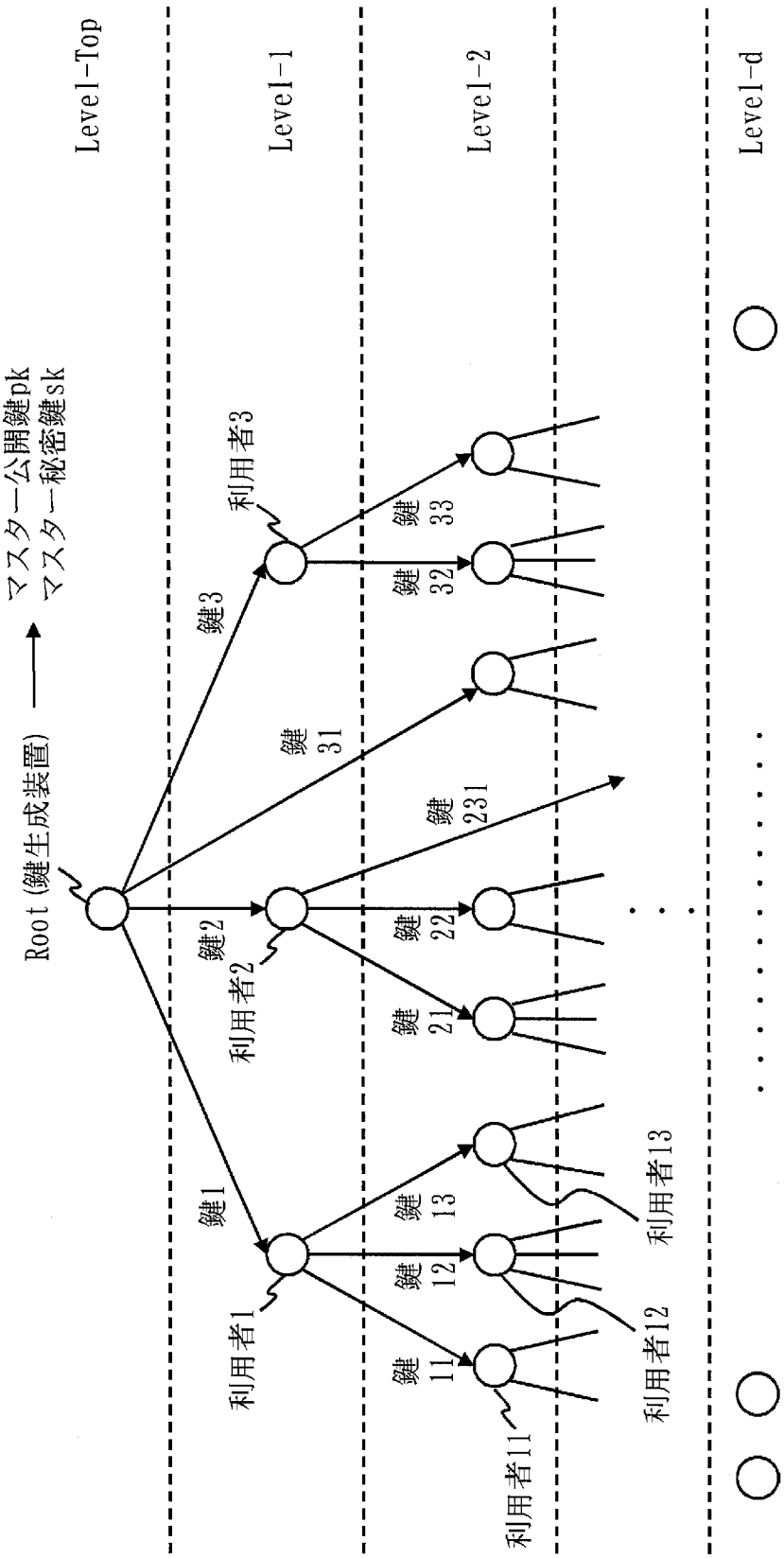
基底B^*_{L+1}の基底ベクトルに述語情報を埋め込んだベクトル$\vec{v}_{L+1}$と、前記復号処理で使用した復号鍵sk_Lとに基づき、前記復号鍵sk_Lの下位の復号鍵sk_{L+1}を生成する鍵委譲処理と

を備えることを特徴とする暗号処理プログラム。

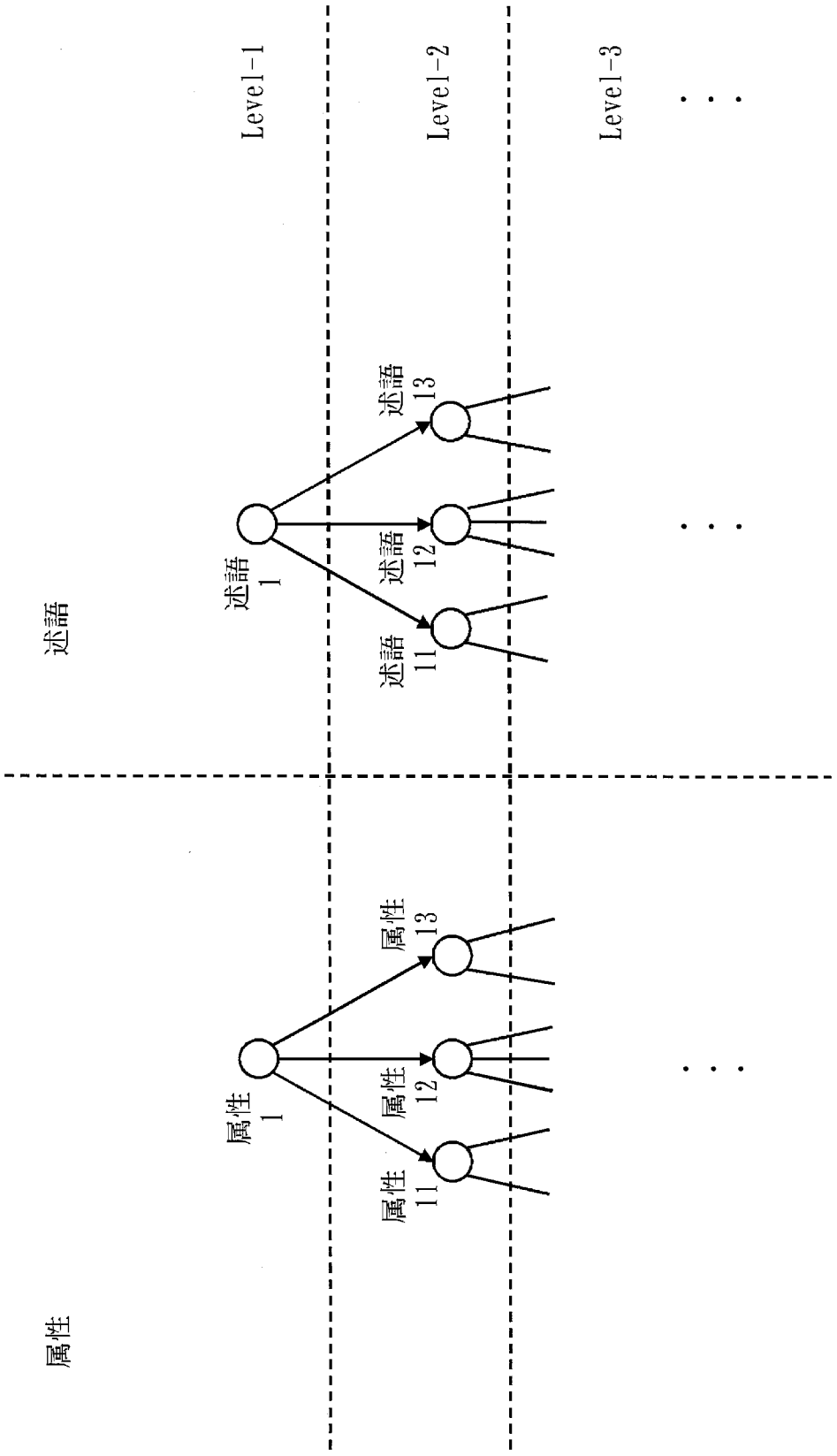
[図1]


Level-Top
Level-1
Level-2
Level-d
マスター公開鍵pk
マスター秘密鍵sk
Root (鍵生成装置)
鍵1
鍵2
鍵3
利用者1
利用者2
利用者3
鍵 11
鍵 12
鍵 13
鍵 21
鍵 22
鍵 23
鍵 31
鍵 32
鍵 33
利用者11
利用者12
利用者13

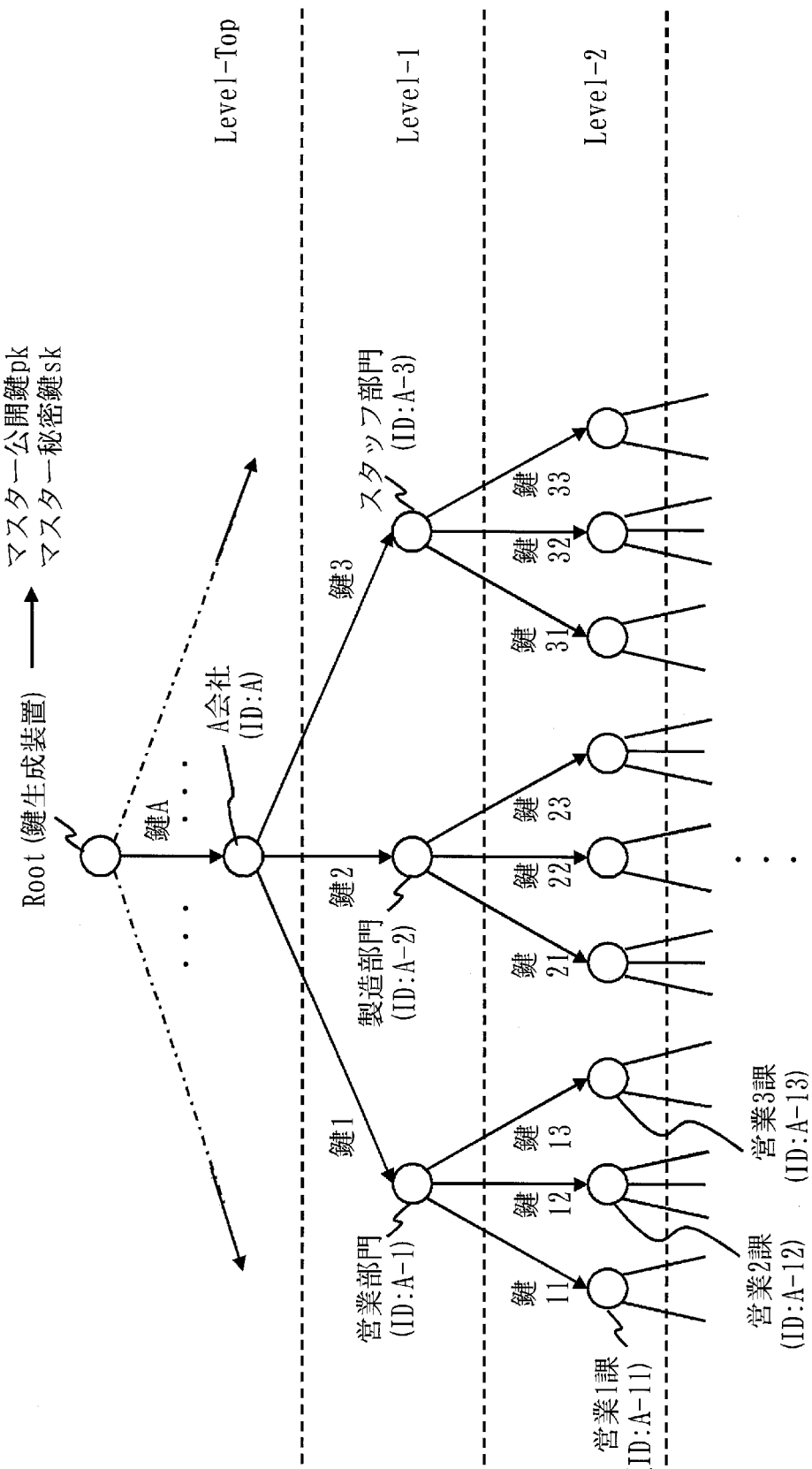
[図2]


Level-Top
Level-1
Level-2
Level-d
マスター公開鍵pk
マスター秘密鍵sk
Root(鍵生成装置)
鍵1
鍵2
鍵3
鍵11
鍵12
鍵13
鍵21
鍵22
鍵231
鍵31
鍵32
鍵33
利用者1
利用者2
利用者3
利用者11
利用者12
利用者13

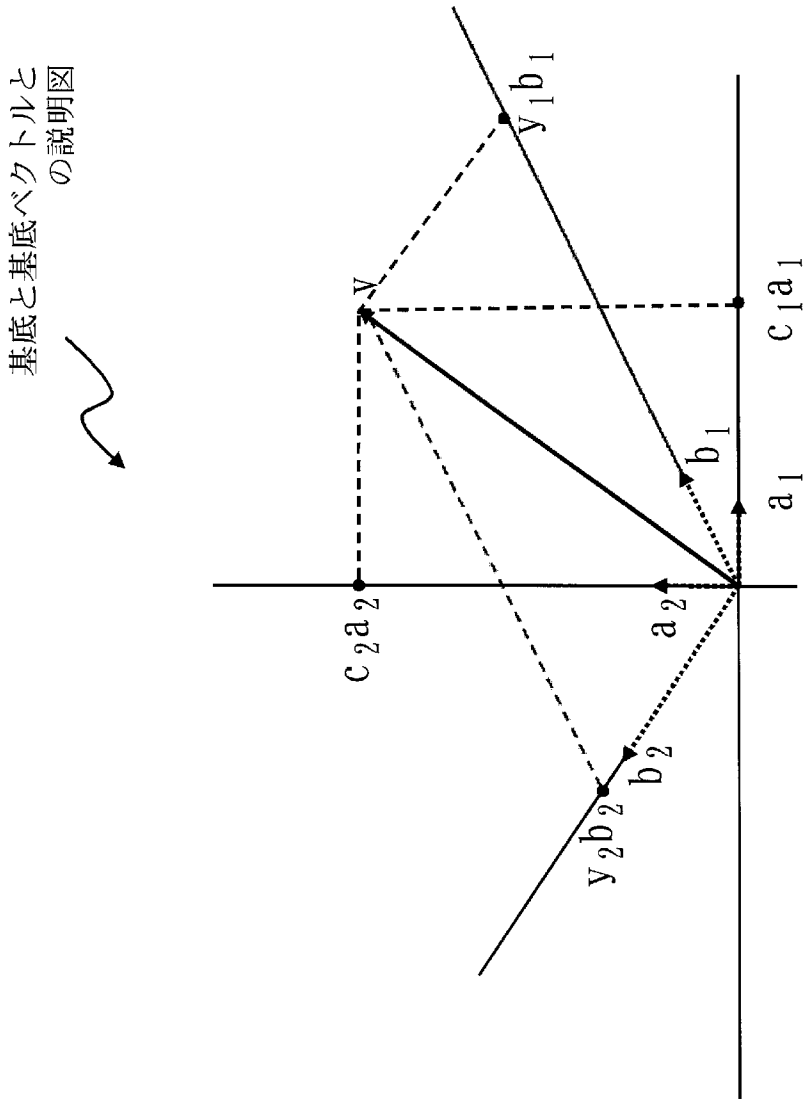
[図3]


Level-1
Level-2
Level-3
述語
述語 1
述語 11
述語 12
述語 13
属性
属性 1
属性 11
属性 12
属性 13

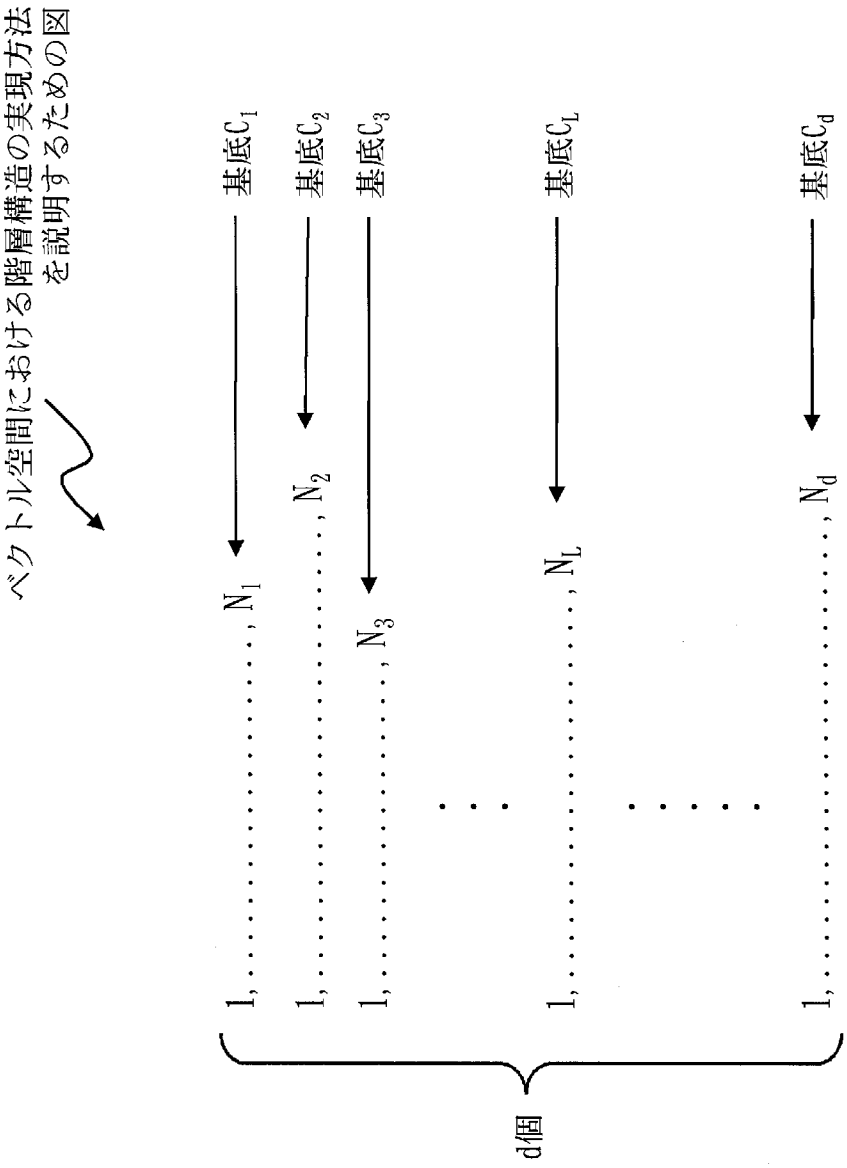
[図4]


Level-Top
Level-1
Level-2
マスター公開鍵pk
マスター秘密鍵sk
Root (鍵生成装置)
鍵A
A会社
(ID:A)
鍵1
営業部門
(ID:A-1)
鍵2
製造部門
(ID:A-2)
鍵3
スタッフ部門
(ID:A-3)
鍵11
鍵12
鍵13
鍵21
鍵22
鍵23
鍵31
鍵32
鍵33
営業1課
(ID:A-11)
営業2課
(ID:A-12)
営業3課
(ID:A-13)

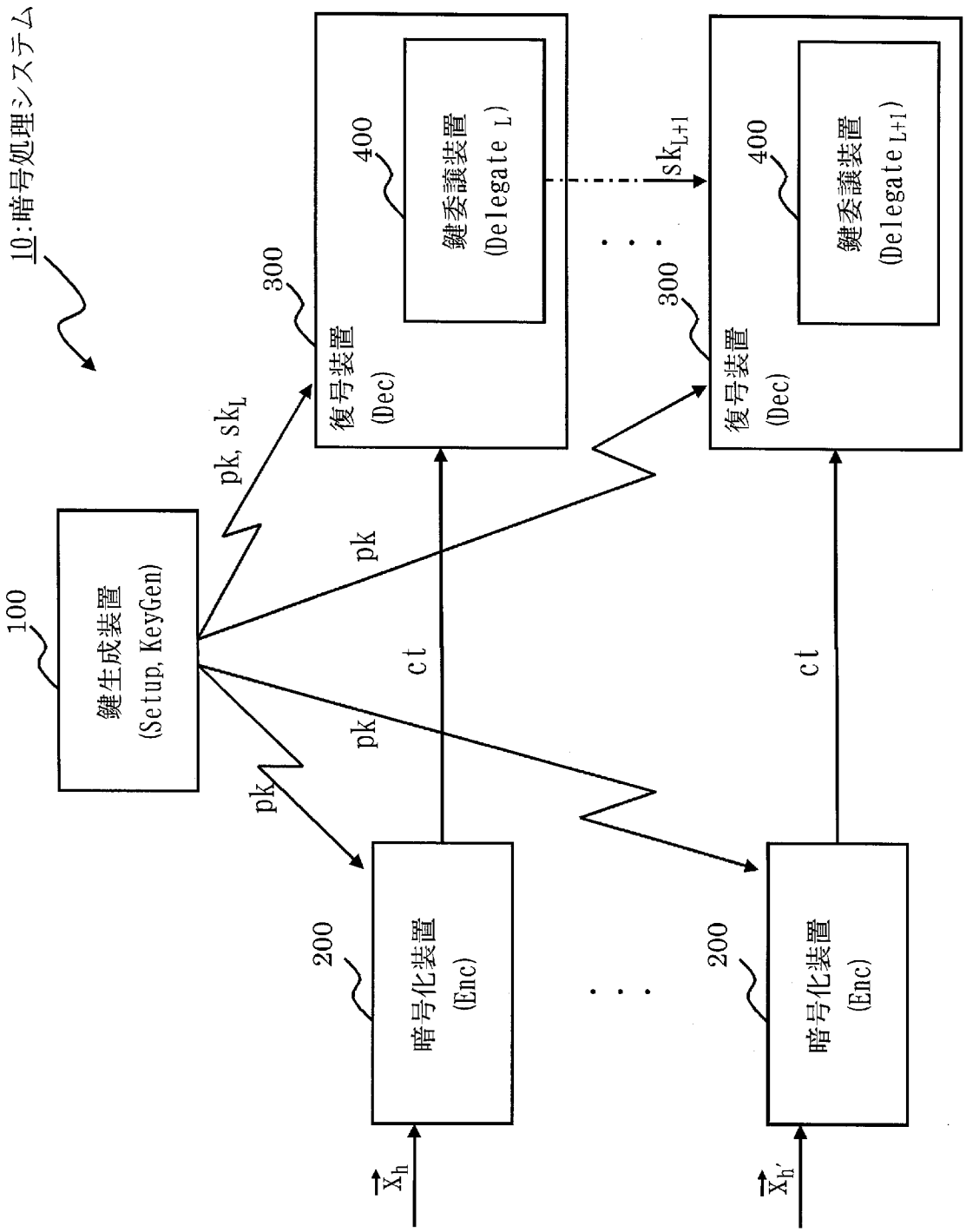
[図5]



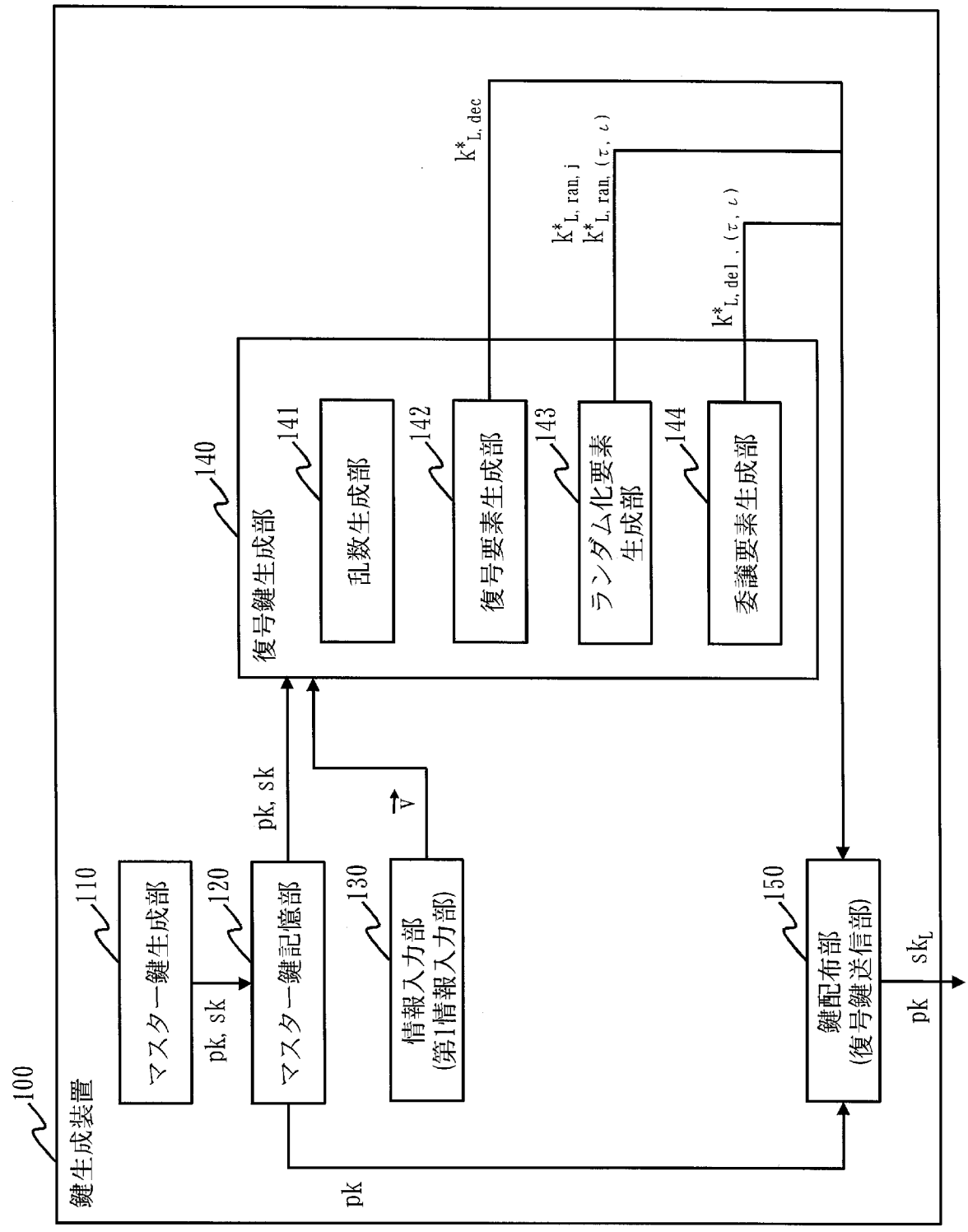
[図6]


ベクトル空間における階層構造の実現方法を説明するための図
基底C_1
基底C_2
基底C_3
基底C_L
基底C_d
1, ... , N_1
1, ... , N_2
1, ... , N_3
1, ... , N_L
1, ... , N_d
d個

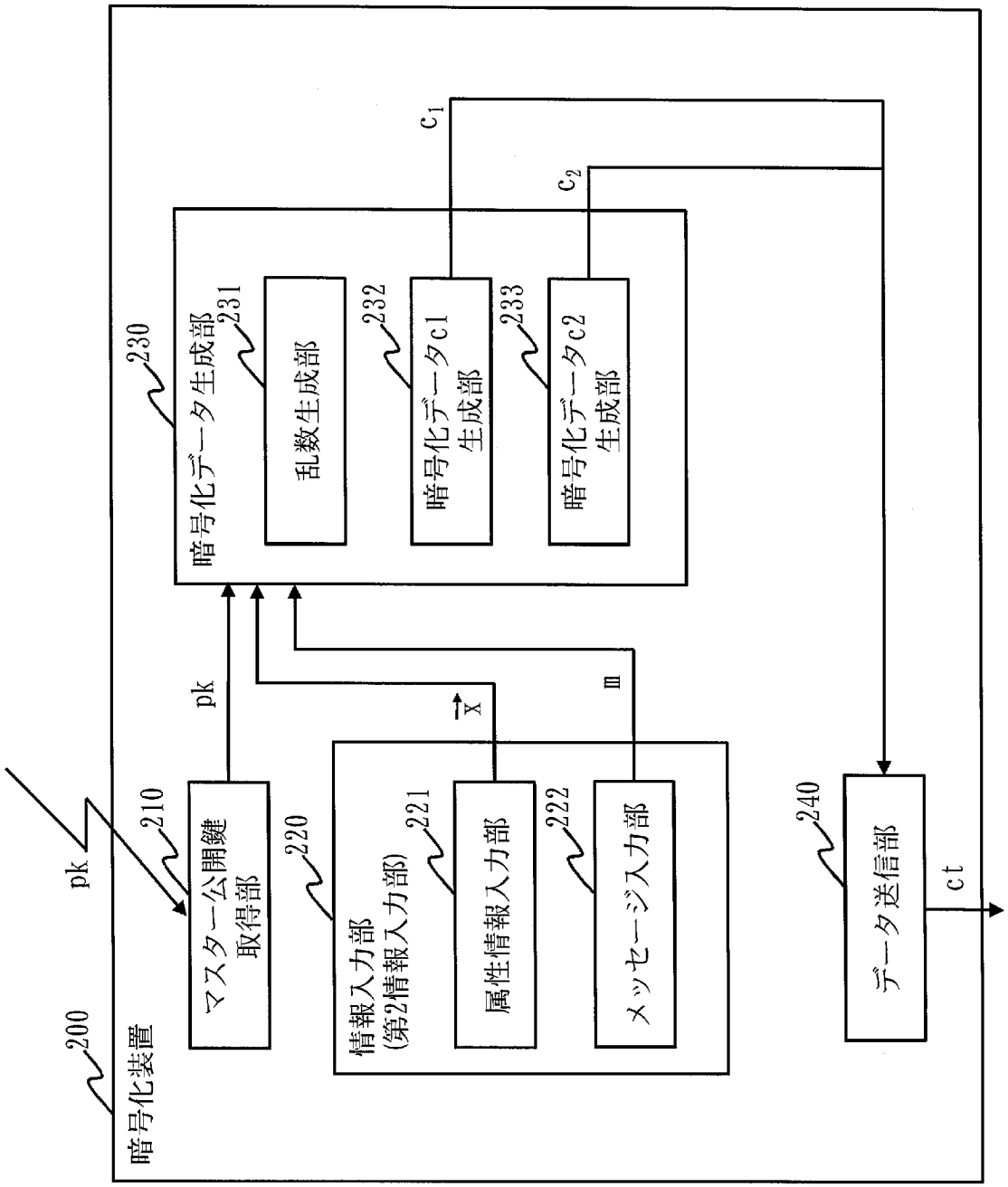
[図7]


10:暗号処理システム
100
鍵生成装置
(Setup, KeyGen)
pk, sk_L
pk
pk
pk
300
復号装置
(Dec)
400
鍵委譲装置
(Delegate_L)
sk_{L+1}
300
復号装置
(Dec)
400
鍵委譲装置
(Delegate_{L+1})
ct
ct
200
暗号化装置
(Enc)
200
暗号化装置
(Enc)
X_h
X_h'

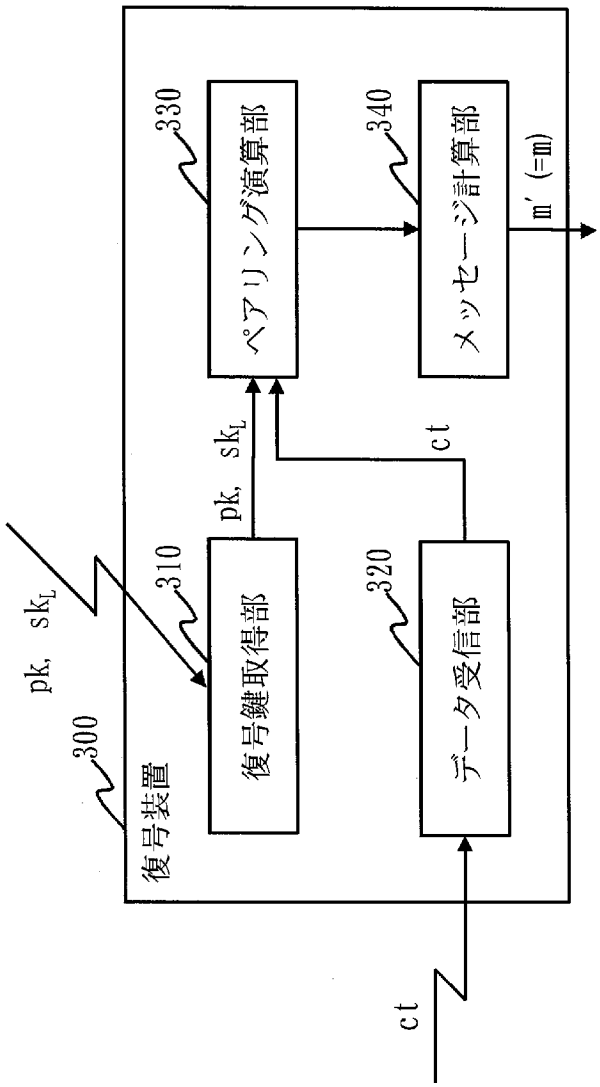
[図8]


鍵生成装置
100
マスター鍵生成部
110
pk, sk
マスター鍵記憶部
120
pk, sk
pk
情報入力部
(第1情報入力部)
130
v
復号鍵生成部
140
乱数生成部
141
復号要素生成部
142
ランダム化要素
生成部
143
委譲要素生成部
144
$k^*_{L,dec}$
$k^*_{L,ran,j}$
$k^*_{L,ran,(\tau,\iota)}$
$k^*_{L,del,(\tau,\iota)}$
鍵配布部
(復号鍵送信部)
150
pk
sk_L

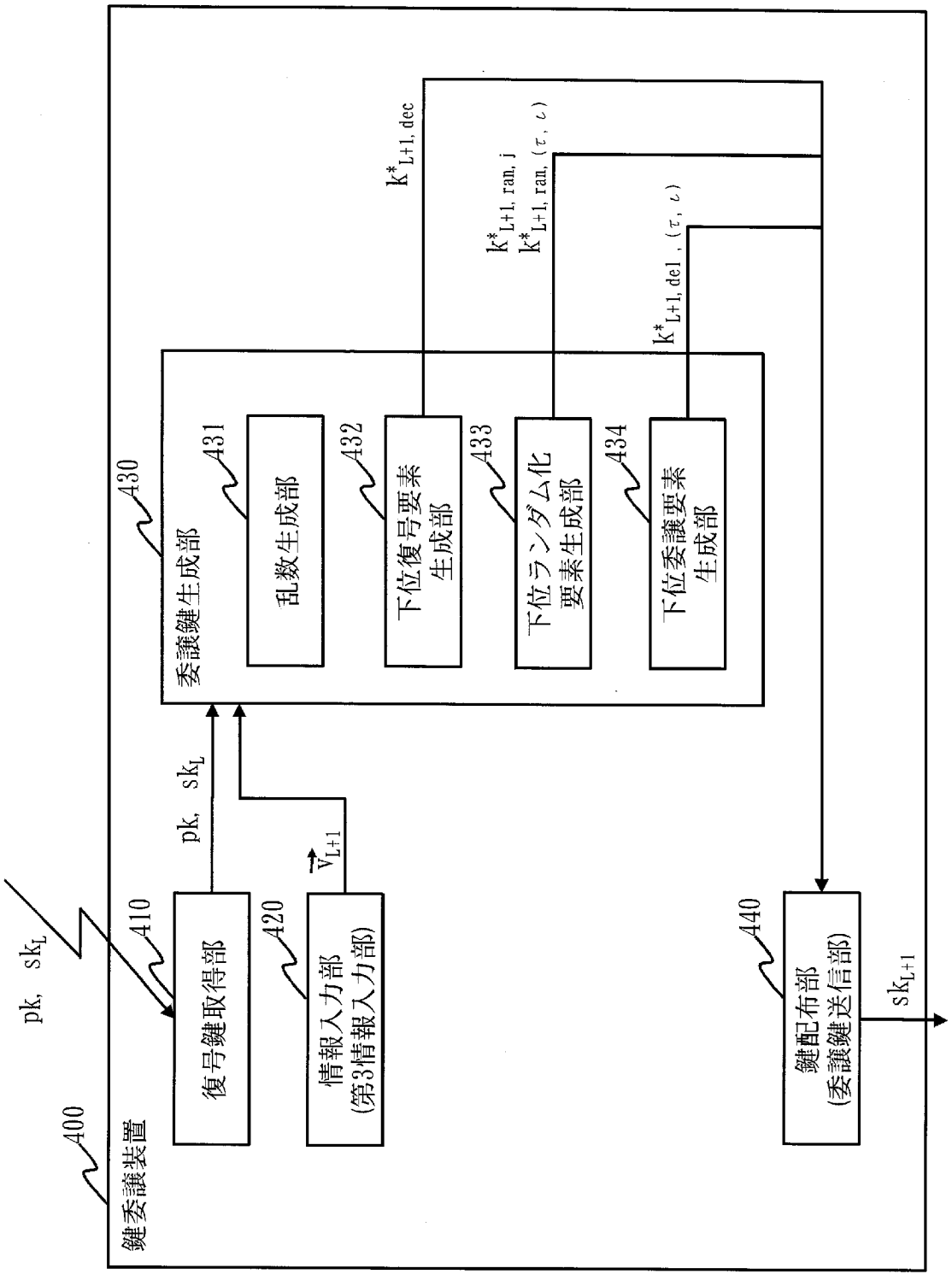
[図9]


200
暗号化装置
pk
210
マスター公開鍵
取得部
pk
220
情報入力部
(第2情報入力部)
221
属性情報入力部
222
メッセージ入力部
x
m
230
暗号化データ生成部
231
乱数生成部
232
暗号化データc1
生成部
233
暗号化データc2
生成部
c1
c2
240
データ送信部
ct

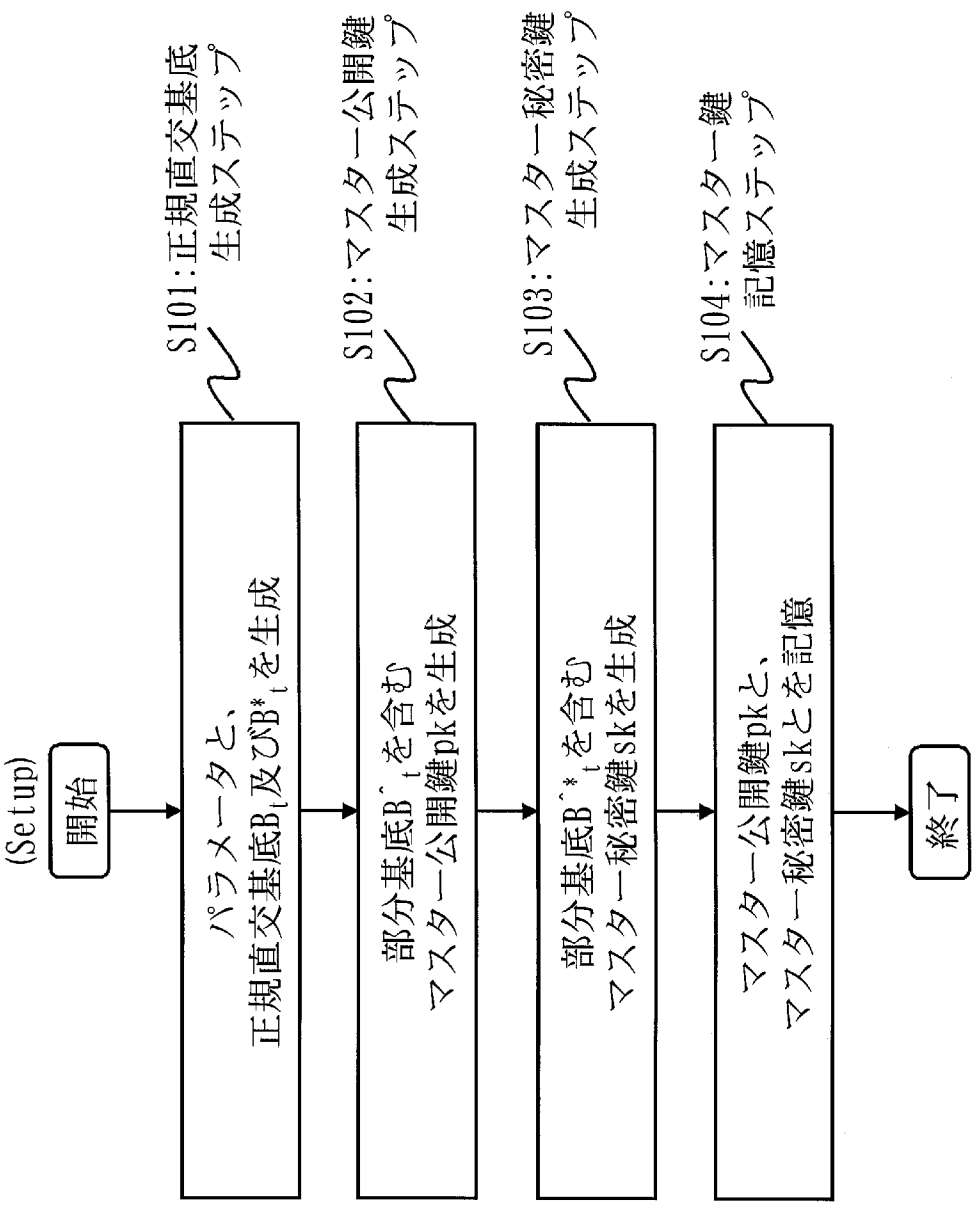
[図10]


復号装置
300
pk, sk_L
310
復号鍵取得部
320
データ受信部
330
ペアリング演算部
340
メッセージ計算部
pk, sk_L
ct
ct
m′(=m)

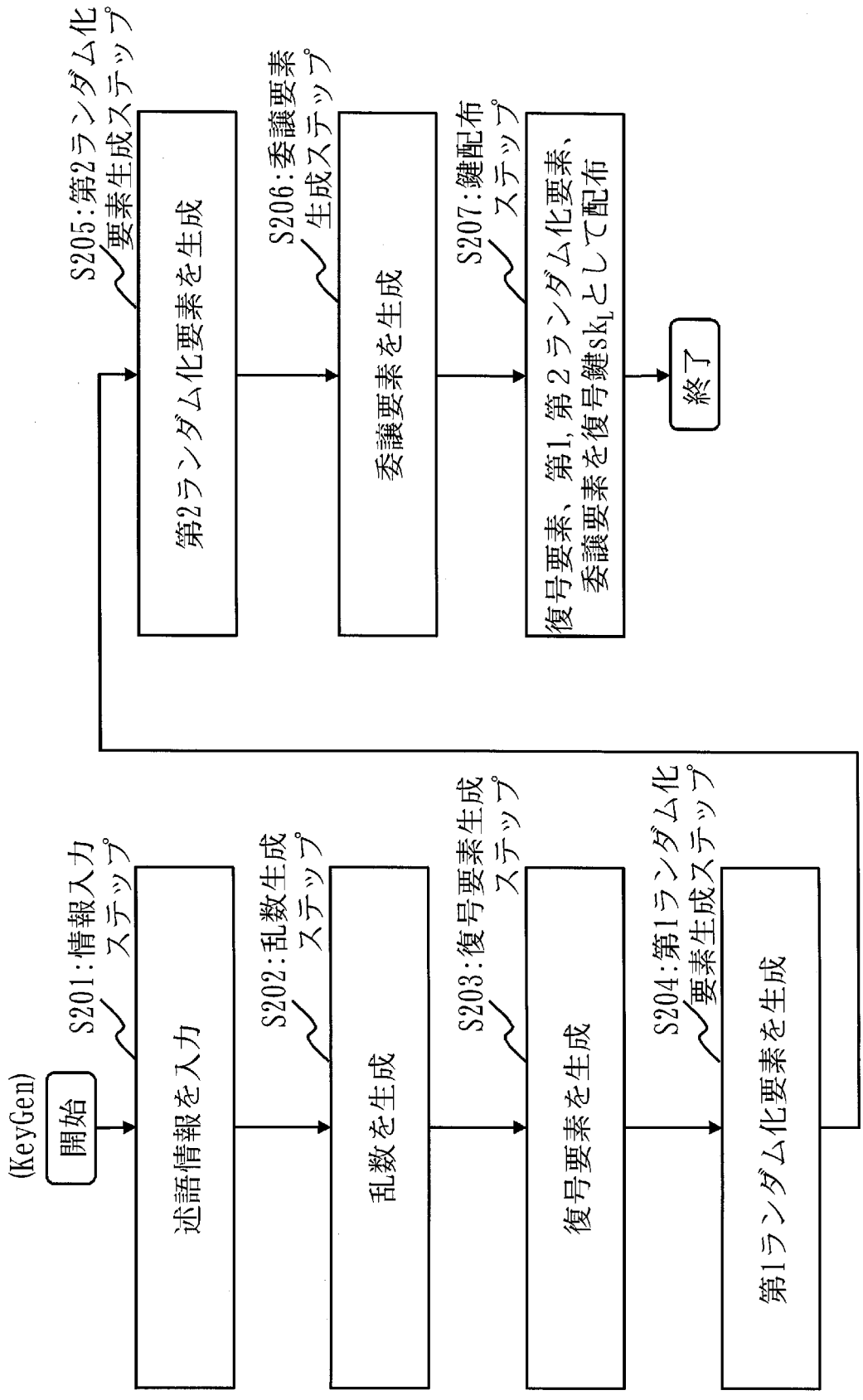
[図11]


鍵委譲装置
400
pk, sk_L
410
復号鍵取得部
420
情報入力部
(第3情報入力部)
pk, sk_L
$\vec{v}_{L+1}$
委譲鍵生成部
430
431
乱数生成部
432
下位復号要素
生成部
433
下位ランダム化
要素生成部
434
下位委譲要素
生成部
$k^*_{L+1,dec}$
$k^*_{L+1,ran,j}$
$k^*_{L+1,ran,(\tau,\iota)}$
$k^*_{L+1,del,(\tau,\iota)}$
440
鍵配布部
(委譲鍵送信部)
sk_{L+1}

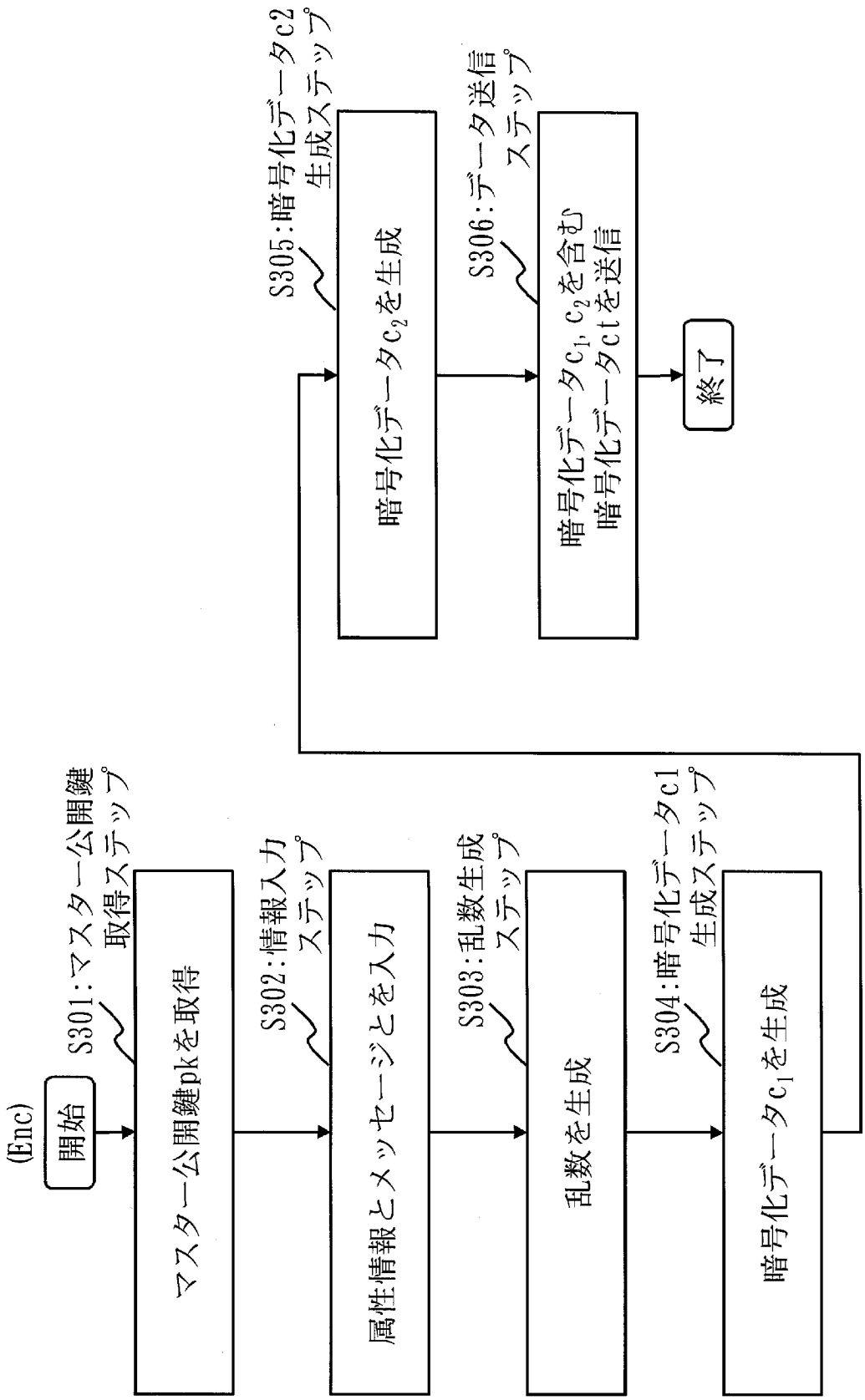
[図12]


(Setup)
開始
S101:正規直交基底
生成ステップ
パラメータと、
正規直交基底B_t及びB^*_tを生成
S102:マスター公開鍵
生成ステップ
部分基底$\hat{B}_t$を含む
マスター公開鍵pkを生成
S103:マスター秘密鍵
生成ステップ
部分基底$\hat{B}^*_t$を含む
マスター秘密鍵skを生成
S104:マスター鍵
記憶ステップ
マスター公開鍵pkと、
マスター秘密鍵skとを記憶
終了

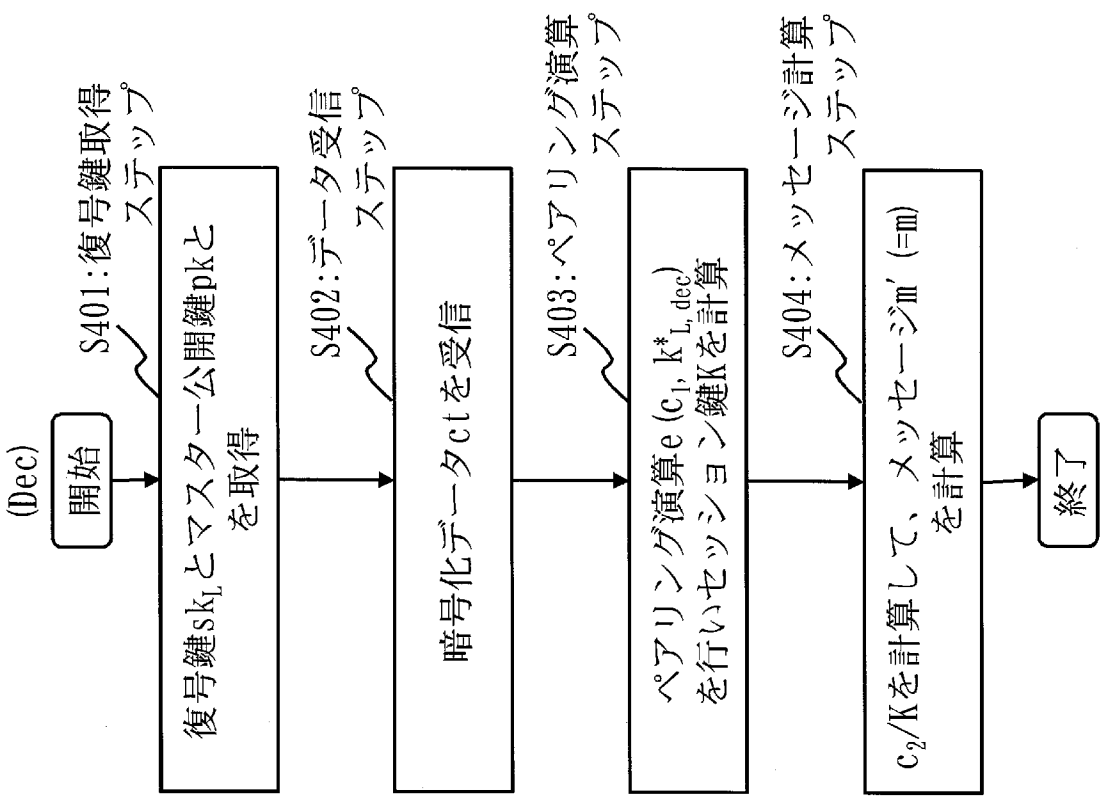
[図13]


(KeyGen)
開始
S201:情報入力ステップ
述語情報を入力
S202:乱数生成ステップ
乱数を生成
S203:復号要素生成ステップ
復号要素を生成
S204:第1ランダム化要素生成ステップ
第1ランダム化要素を生成
S205:第2ランダム化要素生成ステップ
第2ランダム化要素を生成
S206:委譲要素生成ステップ
委譲要素を生成
S207:鍵配布ステップ
復号要素、第1,第2ランダム化要素、委譲要素を復号鍵sk_Lとして配布
終了

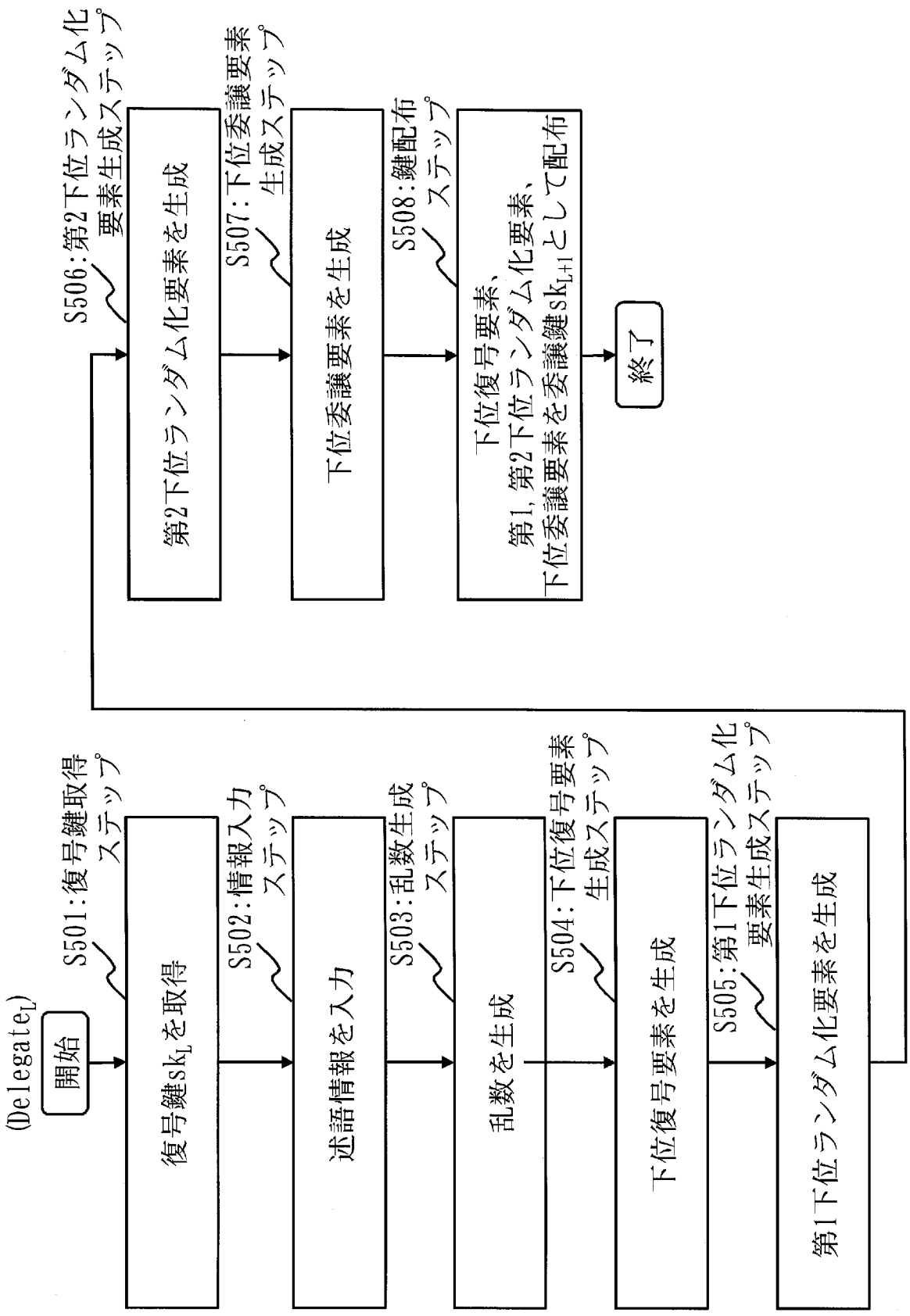
[図14]


(Enc)
開始
S301:マスター公開鍵取得ステップ
マスター公開鍵pkを取得
S302:情報入力ステップ
属性情報とメッセージとを入力
S303:乱数生成ステップ
乱数を生成
S304:暗号化データc1生成ステップ
暗号化データc_1を生成
S305:暗号化データc2生成ステップ
暗号化データc_2を生成
S306:データ送信ステップ
暗号化データc_1, c_2を含む暗号化データctを送信
終了

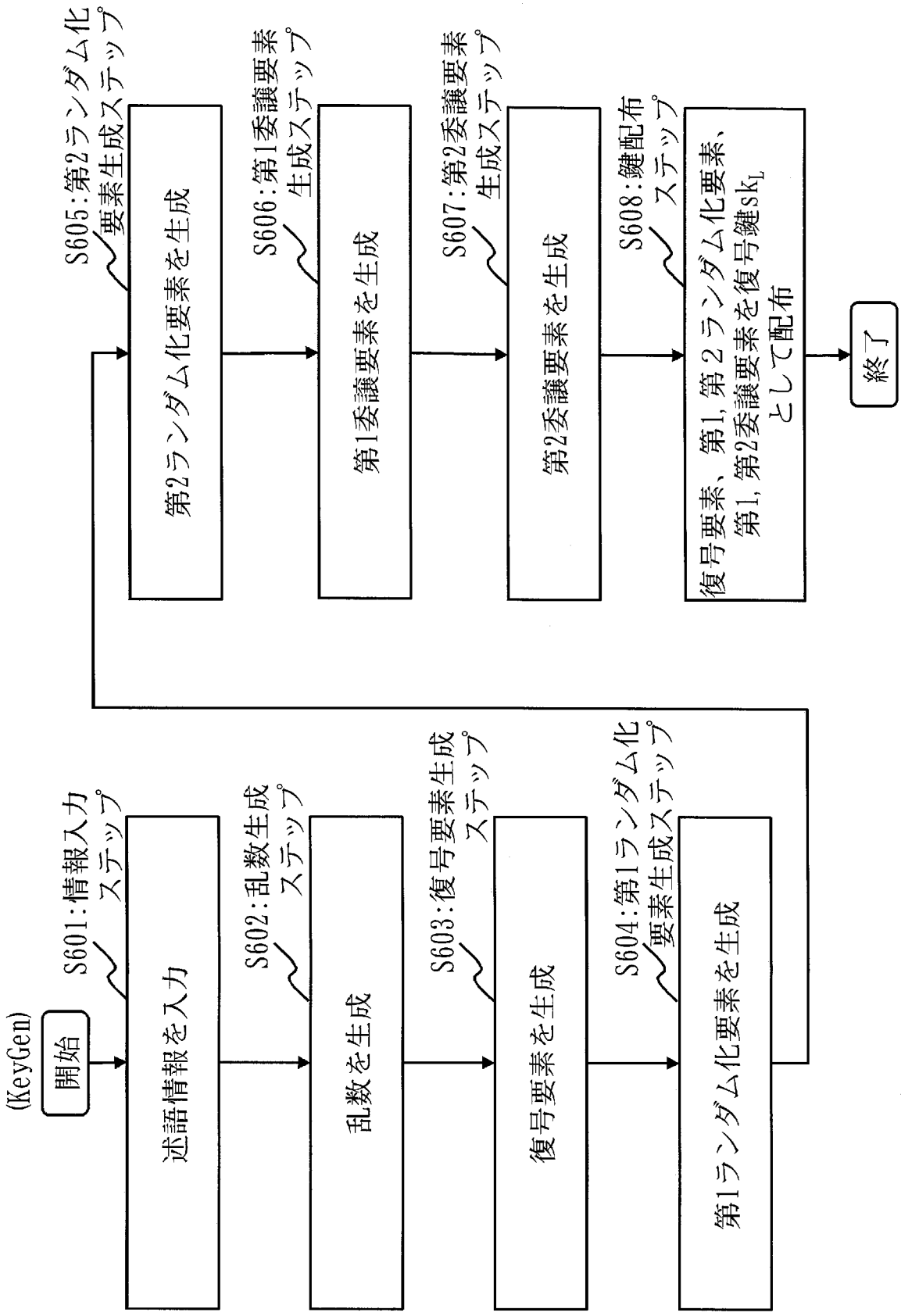
[図15]


(Dec)
開始
S401:復号鍵取得ステップ
復号鍵sk_Lとマスター公開鍵pkと
を取得
S402:データ受信ステップ
暗号化データctを受信
S403:ペアリング演算ステップ
ペアリング演算e (c_1, $k^*_{L,dec}$)
を行いセッション鍵Kを計算
S404:メッセージ計算ステップ
c_2/Kを計算して、メッセージm' (=m)
を計算
終了

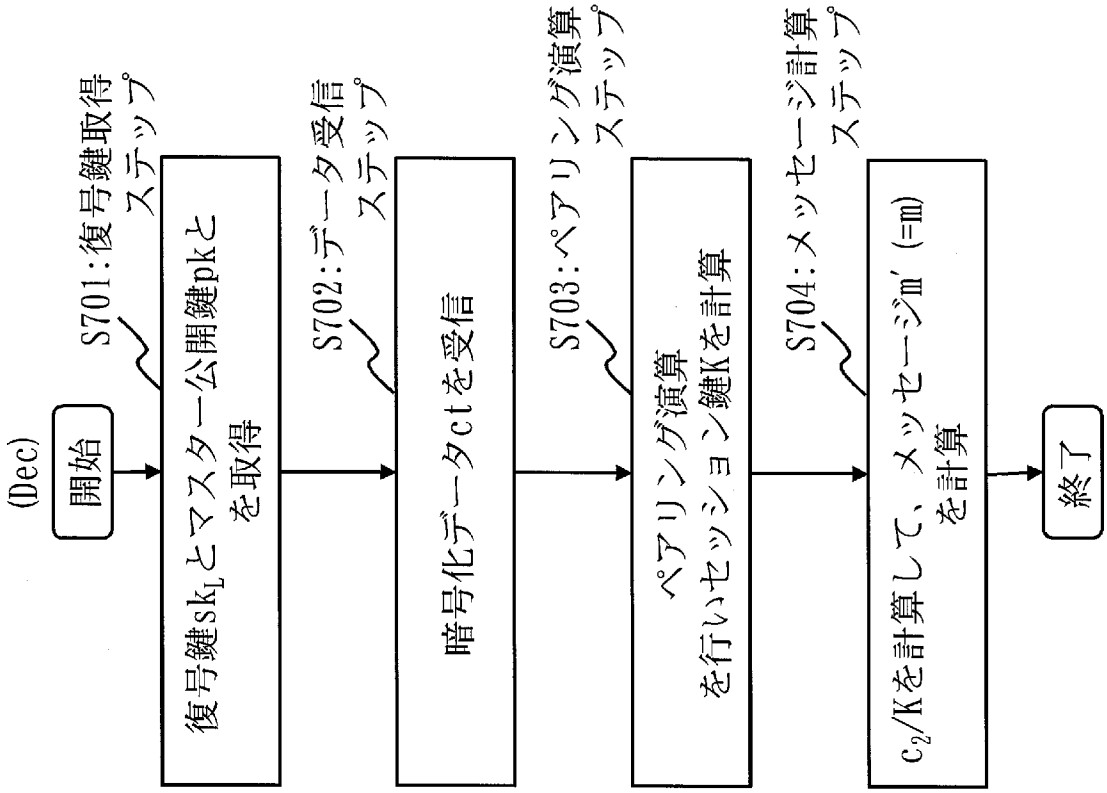
[図16]


(Delegate$_L$)
開始
S501:復号鍵取得ステップ
復号鍵sk_Lを取得
S502:情報入力ステップ
述語情報を入力
S503:乱数生成ステップ
乱数を生成
S504:下位復号要素生成ステップ
下位復号要素を生成
S505:第1下位ランダム化要素生成ステップ
第1下位ランダム化要素を生成
S506:第2下位ランダム化要素生成ステップ
第2下位ランダム化要素を生成
S507:下位委譲要素生成ステップ
下位委譲要素を生成
S508:鍵配布ステップ
下位復号要素、
第1, 第2下位ランダム化要素、
下位委譲要素を委譲鍵sk_{L+1}として配布
終了

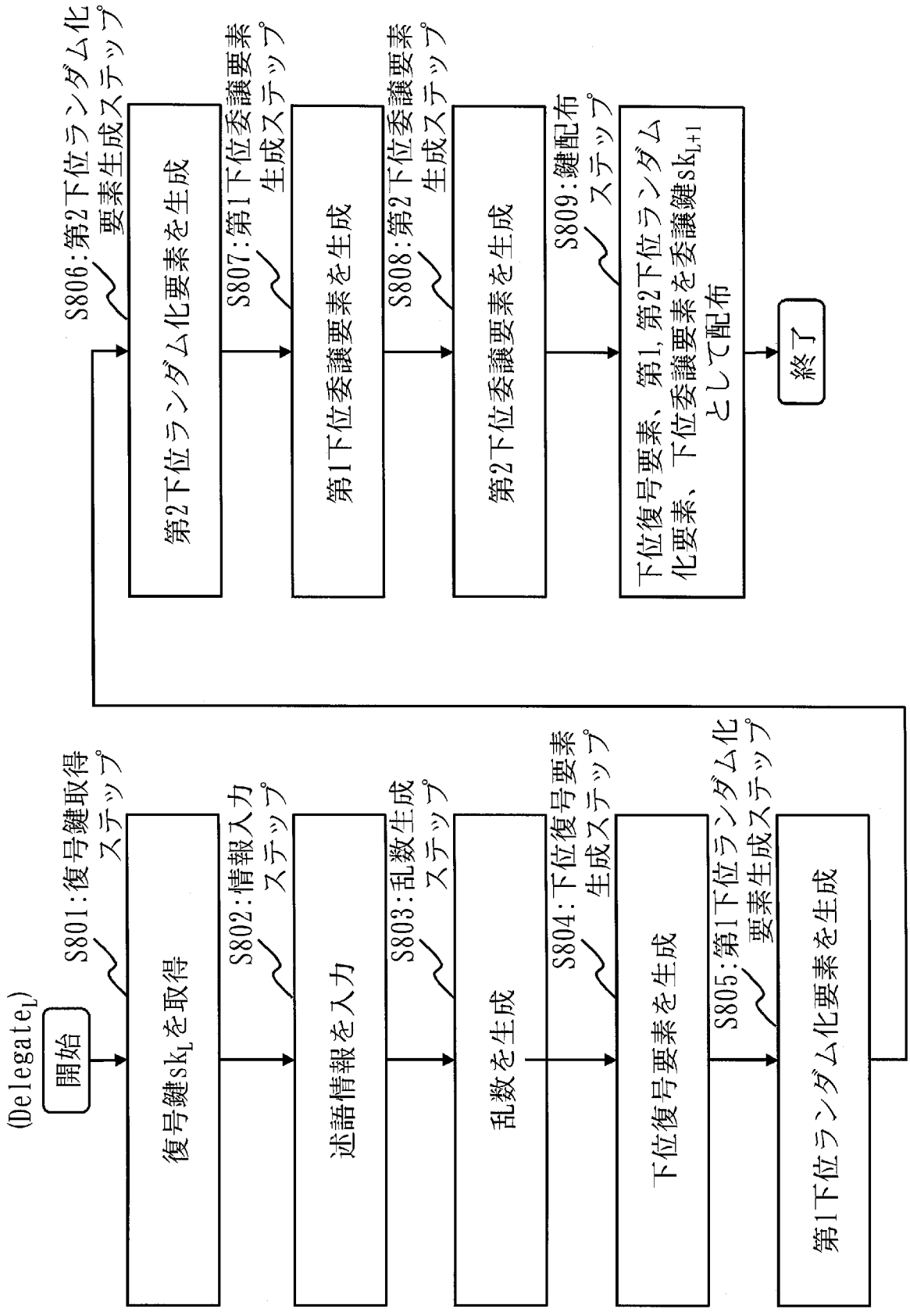
[図17]


(KeyGen)
開始
S601:情報入力ステップ
述語情報を入力
S602:乱数生成ステップ
乱数を生成
S603:復号要素生成ステップ
復号要素を生成
S604:第1ランダム化要素生成ステップ
第1ランダム化要素を生成
S605:第2ランダム化要素生成ステップ
第2ランダム化要素を生成
S606:第1委譲要素生成ステップ
第1委譲要素を生成
S607:第2委譲要素生成ステップ
第2委譲要素を生成
S608:鍵配布ステップ
復号要素、第1, 第2ランダム化要素、第1, 第2委譲要素を復号鍵sk_Lとして配布
終了

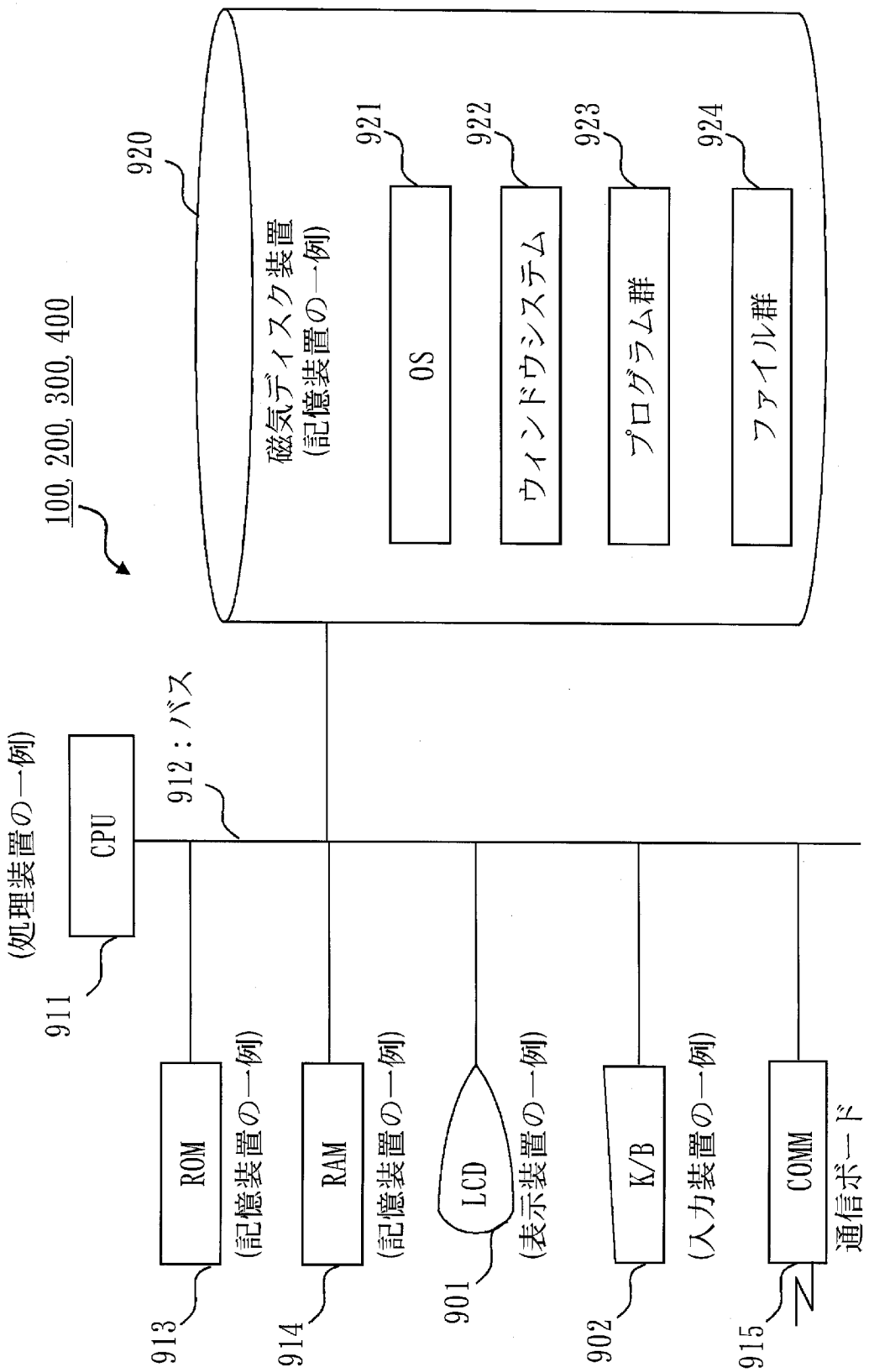
[図18]


(Dec)
開始
S701:復号鍵取得ステップ
復号鍵sk_Lとマスター公開鍵pkと
を取得
S702:データ受信ステップ
暗号化データctを受信
S703:ペアリング演算ステップ
ペアリング演算
を行いセッション鍵Kを計算
S704:メッセージ計算ステップ
c_2/Kを計算して、メッセージm'(=m)
を計算
終了

[図19]


(Delegate$_L$)
開始
S801:復号鍵取得ステップ
復号鍵sk_Lを取得
S802:情報入力ステップ
述語情報を入力
S803:乱数生成ステップ
乱数を生成
S804:下位復号要素生成ステップ
下位復号要素を生成
S805:第1下位ランダム化要素生成ステップ
第1下位ランダム化要素を生成
S806:第2下位ランダム化要素生成ステップ
第2下位ランダム化要素を生成
S807:第1下位委譲要素生成ステップ
第1下位委譲要素を生成
S808:第2下位委譲要素生成ステップ
第2下位委譲要素を生成
S809:鍵配布ステップ
下位復号要素、第1, 第2下位ランダム化要素、下位委譲要素を委譲鍵sk_{L+1}として配布
終了

[図20]


100, 200, 300, 400
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/JP2011/078668

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/30(2006.01)i, *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)
H04L9/30, 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	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII), Predicate Encryption, Functional Encryption, Attribute-Based Encryption, Hierarchical

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 03/081780 A2 (DOCOMO COMMUNICATIONS LABORATORIES USA, INC.), 02 October 2003 (02.10.2003), paragraphs [0068] to [0082]	1-18
A	WO 2008/099831 A1 (NEC Corp.), 21 August 2008 (21.08.2008), paragraphs [0050] to [0069]	1-18
A	US 2009/0080658 A1 (Waters, B. et al.), 26 May 2009 (26.05.2009), paragraphs [0087] to [0104]	1-18
A	US 2009/0225986 A1 (INTERNATIONAL BUSINESS MACHINES CORP.), 10 September 2009 (10.09.2009), paragraphs [0017] to [0045]	1-18

[X] Further documents are listed in the continuation of Box C.

[X] 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 March, 2012 (02.03.12)	13 March, 2012 (13.03.12)

Name and mailing address of the ISA/	Authorized officer
Japanese Patent Office	
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/078668

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/122926 A1 (Mitsubishi Electric Corp., Nippon Telegraph and Telephone Corp.), 28 October 2010 (28.10.2010), paragraphs [0022] to [0025], [0056] to [0091], [0100] to [0141], [0148] to [0209]	1-18
A	Shi, E. and Waters, B., Delegating Capabilities in Predicate Encryption Systems, Lecture Notes in Computer Science, Vol.5126, 2008.07.05, p.560-578, especially 5.1 Construction	1-18
A	Okamoto, T. and Takashima, K., Hierarchical Predicate Encryption for Inner-Products, Lecture Notes in Computer Science, Vol.5912, 2009.12.01, p.214-231, especially 5.2 HPE Scheme	1-18
A	Lewko, A. et al., Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, Lecture Notes in Computer Science, Vol.6110, 2010.05.29, p.62-91, especially 3.5 The Proposed PE Scheme	1-18

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2011/078668

WO 03/081780 A2	2003.10.02	JP 2003-298568 A US 2003/0179885 A1 EP 1495573 B1 DE 60325575 D AU 2003214189 A CN 1633774 A
WO 2008/099831 A1	2008.08.21	US 2010/0020977 A1
US 2009/0080658 A1	2009.05.26	(Family: none)
US 2009/0225986 A1	2009.09.10	(Family: none)
WO 2010/122926 A1	2010.10.28	JP 2010-273317 A US 2012/045056 A1

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０７８６６８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/30(2006.01)i, 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.　H04L9/30, 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	１９７１－２０１２年
日本国実用新案登録公報	１９９６－２０１２年
日本国登録実用新案公報	１９９４－２０１２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）

JSTPlus/JMEDPlus/JST7580(JDreamII) Predicate Encryption, Functional Encryption, Attribute-Based Encryption, Hierarchical

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 03/081780 A2 (DOCOMO COMMUNICATIONS LABORATORIES USA, INC.) 2003.10.02, 68-82 段落	1-18
A	WO 2008/099831 A1 (日本電気株式会社) 2008.08.21, 50-69 段落	1-18
A	US 2009/0080658 A1 (Waters, B. et al.) 2009.05.26, 87-104 段落	1-18
A	US 2009/0225986 A1 (INTERNATIONAL BUSINESS MACHINES CORPORAION) 2009.09.10, 17-45 段落	1-18

☑　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
０２．０３．２０１２	１３．０３．２０１２

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　９３６４
中里　裕正
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
A	WO 2010/122926 A1（三菱電機株式会社, 日本電信電話株式会社）2010.10.28, 22-25, 56-91, 100-141, 148-209 段落	1-18
A	Shi, E. and Waters, B., Delegating Capabilities in Predicate Encryption Systems, Lecture Notes in Computer Science, Vol.5126, 2008.07.05, p.560-578, especially 5.1 Construction	1-18
A	Okamoto, T. and Takashima, K., Hierarchical Predicate Encryption for Inner-Products, Lecture Notes in Computer Science, Vol.5912, 2009.12.01, p.214-231, especially 5.2 HPE Scheme	1-18
A	Lewko, A. et al., Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, Lecture Notes in Computer Science, Vol.6110, 2010.05.29, p.62-91, especially 3.5 The Proposed PE Scheme	1-18

WO 03/081780 A2	2003.10.02	JP 2003-298568 A US 2003/0179885 A1 EP 1495573 B1 DE 60325575 D AU 2003214189 A CN 1633774 A
WO 2008/099831 A1	2008.08.21	US 2010/0020977 A1
US 2009/0080658 A1	2009.05.26	ファミリーなし
US 2009/0225986 A1	2009.09.10	ファミリーなし
WO 2010/122926 A1	2010.10.28	JP 2010-273317 A US 2012/045056 A1