(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 6 月 28 日(28.06.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/086405 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2011/078164

(22) 国際出願日: 2011 年 12 月 6 日(06.12.2011)

(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 2010-286511 2010 年 12 月 22 日(22.12.2010) 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.

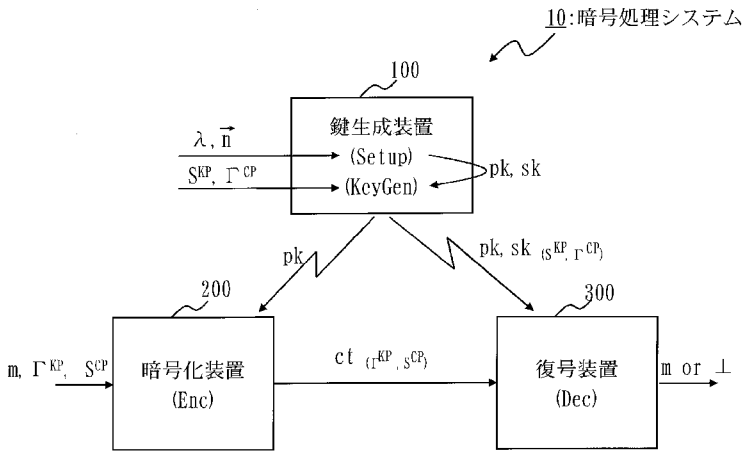
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, 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, 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、暗号処理方法及び暗号処理プログラム

[図5]



10 ENCRYPTION PROCESSING SYSTEM
100 KEY GENERATION DEVICE
200 ENCRYPTION DEVICE
300 DECRYPTION DEVICE

(57) **Abstract**: An objective of the present invention is to provide a secure functional encryption scheme having many encryption functions. Configured is an access structure by applying inner products of characteristic vectors to a span program. The access structure has degrees of freedom in span program design and characteristic vector design, and comprises a large degree of freedom in the design of access control. Respectively assigning the access structure to the encrypted text and the decryption key implements the functional encryption scheme.

(57) 要約: 多くの暗号機能を有する安全な関数型暗号方式を提供することを目的とする。スパンプログラムに属性ベクトルの内積を適用することにより、アクセスストラクチャを構成した。このアクセスストラクチャは、スパンプログラムの設計と、属性ベクトルの設計とに自由度があり、アクセス制御の設計に大きな自由度を有する。このアクセスストラクチャを、暗号文と復号鍵とのそれぞれに持たせて関数型暗号処理を実現した。

WO 2012/086405 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

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、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、関数型暗号（Ｆｕｎｃｔｉｏｎａｌ　Ｅｎｃｒｙｐｔｉｏｎ，ＦＥ）方式に関するものである。

背景技術

[0002] 非特許文献３－６，１０，１２，１３，１５，１８には、関数型暗号方式の１つのクラスであるＩＤベース暗号（Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ，ＩＢＥ）方式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．：Ｃｉｐｈｅｒｔｅｘｔｐｏｌｉｃｙ 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 ｂａｓｅｄ 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.) CRYPTO2001. 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 crypto

systems 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. EUROCRYPT2004, 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.) IMAInt. Conf. LNCS, vol. 2260, pp. 360-63. Springer Heidelberg (2001)

非特許文献13：Gentry, C.: Practical identity-based encryption without rando

m 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 controlof encrypted data. In: ACM Conference on Computer and Communication Security 2006, pp. 89-8, ACM (2006)

非特許文献17：Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N. P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415-32. Springer Heidelberg (2008)

非特許文献18：Ｈｏｒｗｉｔｚ，Ｊ．，Ｌｙｎｎ，Ｂ．：Ｔｏｗａｒｄｓ ｈｉｅｒａｒｃｈｉｃａｌ ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ ｅｎｃｒｙｐｔｉｏｎ．Ｉｎ：Ｋｎｕｄｓｅｎ，Ｌ．Ｒ．（ｅｄ．）ＥＵＲＯＣＲＹＰＴ ２００２．ＬＮＣＳ，ｖｏｌ．２３３２，ｐｐ．４６６･８１．Ｓｐｒｉｎｇｅｒ Ｈｅｉｄｅｌｂｅｒｇ（２００２）

非特許文献19：Ｋａｔｚ，Ｊ．，Ｓａｈａｉ，Ａ．，Ｗａｔｅｒｓ，Ｂ．：Ｐｒｅｄｉｃａｔｅ ｅｎｃｒｙｐｔｉｏｎ ｓｕｐｐｏｒｔｉｎｇ ｄｉｓｊｕｎｃｔｉｏｎｓ，ｐｏｌｙｎｏｍｉａｌ ｅｑｕａｔｉｏｎｓ，ａｎｄｉｎｎｅｒ ｐｒｏｄｕｃｔｓ．Ｉｎ：Ｓｍａｒｔ，Ｎ．Ｐ．（ｅｄ．）ＥＵＲＯＣＲＹＰＴ ２００８．ＬＮＣＳ，ｖｏｌ．４９６５，ｐｐ．１４６･６２．Ｓｐｒｉｎｇｅｒ Ｈｅｉｄｅｌｂｅｒｇ（２００８）

非特許文献20：Ｌｅｗｋｏ，Ａ．，Ｏｋａｍｏｔｏ，Ｔ．，Ｓａｈａｉ，Ａ．，Ｔａｋａｓｈｉｍａ，Ｋ．，Ｗａｔｅｒｓ，Ｂ．：Ｆｕｌｌｙ ｓｅｃｕｒｅ ｆｕｎｃｔｉｏｎａｌ ｅｎｃｒｙｐｔｉｏｎ：Ａｔｔｒｉｂｕｔｅ－ｂａｓｅｄ ｅｎｃｒｙｐｔｉｏｎ ａｎｄ（ｈｉｅｒａｒｃｈｉｃａｌ）ｉｎｎｅｒ ｐｒｏｄｕｃｔ ｅｎｃｒｙｐｔｉｏｎ，Ｉｎ：Ｇｉｌｂｅｒｔ，Ｈ．（ｅｄ．）ＥＵＲＯＣＲＹＰＴ ２０１０．ＬＮＣＳ，ｖｏｌ．６１１０，ｐｐ．６２－９１．Ｓｐｒｉｎｇｅｒ，Ｈｅｉｄｅｌｂｅｒｇ（２０１０）

非特許文献21：Ｌｅｗｋｏ，Ａ．Ｂ．，Ｗａｔｅｒｓ，Ｂ．：Ｆｕｌｌｙ ｓｅｃｕｒｅ ＨＩＢＥ ｗｉｔｈ ｓｈｏｒｔ ｃｉｐｈｅｒｔｅｘｔｓ．ｅＰｒｉｎｔ，ＩＡＣＲ，ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ／２００９／４８２

非特許文献22：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23：Okamoto, T., Takashima, K.: Hierarchical predicate encryption for Inner−Products, In: ASIACRYPT 2009, Springer Heidelberg (2009)

非特許文献24：Okamoto, T., Takashima, K.: Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, In: CRYPTO 2010, LNCS vol. 6223, pp. 191−208. Springer Heidelberg (2010)

非特許文献25：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26：Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute−based systems. In: ACM Conferenceon Computer and Communication Security 2006, pp. 99･12, ACM, (2006)

非特許文献27：Sahai, A., Waters, B.: Fuzzy identity−based encryption. In: C

ramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457･73. Springer Heidelberg (2005)

非特許文献28：Shi, E., Waters, B.: Delegating capability in predicate encryption systems. In: Aceto, L., Damgard, I., Goldberg, L. A., Halldosson, M. M., Ingofsdotir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, pp. 560･78. Springer Heidelberg (2008)

非特許文献29：Waters, B.: Efficient identity based encryption without random oracles. Eurocrypt 2005, LNCS No. 3152, pp. 443･59. Springer Verlag, 2005.

非特許文献30：Waters, B.: Ciphertext－policy attribute－based encryption: an expressive, efficient, and provably securerealization. ePrint, IACR, http://eprint.iacr.org/2008/290

非特許文献31：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] この発明は、多機能な暗号機能を有する安全な関数型暗号方式を提供することを目的とする。

課題を解決するための手段

[0005] この発明に係る暗号処理システムは、

鍵生成装置と暗号化装置と復号装置とを備え、基底B_0及び基底B_0^*と、$t=1,\ldots,d^{KP}$（d^{KP}は１以上の整数）の各整数tについての基底B_t^{KP}及び基底$B^*_t{}^{KP}$と、$t=1,\ldots,d^{CP}$（d^{CP}は１以上の整数）の各整数tについての基底B_t^{CP}及び基底$B^*_t{}^{CP}$とを用いて暗号処理を実行する暗号処理システムであり、

前記鍵生成装置は、

$i=1,\ldots,L^{KP}$（L^{KP}は１以上の整数）の各整数iについての変数$\rho^{KP}(i)$であって、識別情報t（$t=1,\ldots,d^{KP}$のいずれかの整数）と、属性ベクトル$\vec{v}_i^{KP}:=(v_{i,i'}{}^{KP})$（$i'=1,\ldots,n_t^{KP}$，$n_t^{KP}$は１以上の整数）との肯定形の組$(t,\vec{v}_i^{KP})$又は否定形の組$\neg(t,\vec{v}_i^{KP})$のいずれかである変数$\rho^{KP}(i)$と、$L^{KP}$行$r^{KP}$列（$r^{KP}$は１以上の整数）の所定の行列$M^{KP}$とを入力する第１ＫＰ情報入力部と、

$t=1,\ldots,d^{CP}$の少なくとも１つ以上の整数tについて、識別情報tと、属性ベクトル$\vec{x}_t^{CP}:=(x_{t,i'}{}^{CP})$（$i'=1,\ldots,n_t^{CP}$，$n_t^{CP}$は１以上の整数）とを有する属性集合$\Gamma^{CP}$を入力する第１ＣＰ情報入力部と、

基底B^*_0の基底ベクトル$b^*_{0,p}$（pは所定の値）の係数として値$-s_0^{KP}$（$s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$，$\vec{h}^{KP}$及び$\vec{f}^{KP}$は$r^{KP}$個の要素を有するベクトル）を設定し、基底ベクトル$b^*_{0,p'}$（$p'$は前記$p$とは異なる所定の値）の係数として乱数$\delta^{CP}$を設定し、基底ベクトル$b^*_{0,q}$（$q$は前記$p$及び前記$p'$とは異なる所定の値）の係数として所定の値$\kappa$を設定して要素$k^*_0$を生成する主復号鍵生成部と、

前記$\vec{f}^{KP}$と、前記第１ＫＰ情報入力部が入力した行列M^{KP}に基づき生成さ

れる列ベクトル（$s^{\rightarrow KP}$）^{T}：＝（s_{1}^{KP}，．．．，s_{i}^{KP}）^{T}：＝M^{KP}・（$f^{\rightarrow KP}$）^{T}（ｉ＝L^{KP}）と、乱数θ_{i}^{KP}（ｉ＝１，．．．，L^{KP}）とに基づき、ｉ＝１，．．．，L^{KP}の各整数ｉについての要素$k^{*}{}_{i}^{KP}$を生成するＫＰ復号鍵生成部であって、ｉ＝１，．．．，L^{KP}の各整数ｉについて、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$v^{\rightarrow}{}_{i}^{KP}$）である場合には、その組の識別情報ｔが示す基底$B^{*}{}_{t}^{KP}$の基底ベクトル$b^{*}{}_{t,1}^{KP}$の係数として$s_{i}^{KP}+\theta_{i}^{KP}v_{i,1}^{KP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，n_{t}^{KP}の各整数ｉ’とが示す基底ベクトル$b^{*}{}_{t,i'}^{KP}$の係数として$\theta_{i}^{KP}v_{i,i'}^{KP}$を設定して要素$k^{*}{}_{i}^{KP}$を生成し、変数$\rho^{KP}$（ｉ）が否定形の組¬（ｔ，$v^{\rightarrow}{}_{i}^{KP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，n_{t}^{KP}の各整数ｉ’とが示す基底ベクトル$b^{*}{}_{t,i'}^{KP}$の係数として$s_{i}^{KP}v_{i,i'}^{KP}$を設定して要素$k^{*}{}_{i}^{KP}$を生成するＫＰ復号鍵生成部と、

前記第１ＣＰ情報入力部が入力した属性集合Γ^{CP}に含まれる各識別情報ｔについての要素$k^{*}{}_{t}^{CP}$を生成するＣＰ復号鍵生成部であって、基底$B^{*}{}_{t}^{CP}$の基底ベクトル$b^{*}{}_{t,i'}^{CP}$（ｉ’＝１，．．．，n_{t}^{CP}）の係数として前記乱数δ^{CP}倍した$x_{t,i'}^{CP}$を設定して要素$k^{*}{}_{t}^{CP}$を生成するＣＰ復号鍵生成部とを備え、

前記暗号化装置は、

ｔ＝１，．．．，d^{KP}の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$x^{\rightarrow}{}_{t}^{KP}$：＝（$x_{t,i'}^{KP}$）（ｉ’＝１，．．．，$n_{t}^{KP}$）とを有する属性集合$\Gamma^{KP}$を入力する第２ＫＰ情報入力部と、

ｉ＝１，．．．，L^{CP}（L^{CP}は１以上の整数）の各整数ｉについての変数ρ^{CP}（ｉ）であって、識別情報ｔ（ｔ＝１，．．．，d^{CP}のいずれかの整数）と、属性ベクトル$v^{\rightarrow}{}_{i}^{CP}$：＝（$v_{i,i'}^{CP}$）（ｉ’＝１，．．．，$n_{t}^{CP}$）との肯定形の組（ｔ，$v^{\rightarrow}{}_{i}^{CP}$）又は否定形の組¬（ｔ，$v^{\rightarrow}{}_{i}^{CP}$）のいずれかである変数$\rho^{CP}$（ｉ）と、$L^{CP}$行$r^{CP}$列（$r^{CP}$は１以上の整数）の所定の行列$M^{CP}$とを入力する第２ＣＰ情報入力部と、

基底B_{0}の基底ベクトル$b_{0,p}$の係数として乱数ω^{KP}を設定し、基底ベクト

ルｂ$_{0,p'}$の係数として値－ｓ$_0^{CP}$（ｓ$_0^{CP}$：＝ｈ$^{\rightarrow CP}$・（ｆ$^{\rightarrow CP}$）^{T}，ｈ$^{\rightarrow CP}$及びｆ$^{\rightarrow CP}$はｒ^{CP}個の要素を有するベクトル）を設定し、基底ベクトルｂ$_{0,q}$の係数として乱数ζを設定して要素ｃ$_0$を生成する主暗号化データ生成部と、

前記第２ＫＰ情報入力部が入力した属性集合Γ^{KP}に含まれる各識別情報ｔについての要素ｃ$_t^{KP}$を生成するＫＰ暗号化データ生成部であって、基底Ｂ$_t^{KP}$の基底ベクトルｂ$_{t,i',KP}$（ｉ’＝１，．．．，ｎ$_t$）の係数として前記乱数ω^{KP}倍したｘ$_{t,i',KP}$を設定して要素ｃ$_t^{KP}$を生成するＫＰ暗号化データ生成部と、

前記ｆ$^{\rightarrow CP}$と、前記第２ＣＰ情報入力部が入力した行列Ｍ^{CP}とに基づき生成される列ベクトル（ｓ$^{\rightarrow CP}$）^{T}：＝（ｓ$_1^{CP}$，．．．，ｓ$_i^{CP}$）^{T}：＝Ｍ^{CP}・（ｆ$^{\rightarrow CP}$）^{T}（ｉ＝Ｌ^{CP}）と、乱数θ$_i^{CP}$（ｉ＝１，．．．，Ｌ^{CP}）とに基づき、ｉ＝１，．．．，Ｌ^{CP}の各整数ｉについての要素ｃ$_i^{CP}$を生成するＣＰ暗号化データ生成部であって、ｉ＝１，．．．，Ｌ^{CP}の各整数ｉについて、変数ρ^{CP}（ｉ）が肯定形の組（ｔ，ｖ$^{\rightarrow}{}_i^{CP}$）である場合には、その組の識別情報ｔが示す基底Ｂ$_t^{CP}$の基底ベクトルｂ$_{t,1}^{CP}$の係数としてｓ$_i^{CP}$＋θ$_i^{CP}$ｖ$_{i,1}^{CP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，ｎ$_t^{CP}$の各整数ｉ’とが示す基底ベクトルｂ$_{t,i',CP}$の係数としてθ$_i^{CP}$ｖ$_{i,i',CP}$を設定して要素ｃ$_i^{CP}$を生成し、変数ρ^{CP}（ｉ）が否定形の組￢（ｔ，ｖ$^{\rightarrow}{}_i^{CP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，ｎ$_t^{CP}$の各整数ｉ’とが示す基底ベクトルｂ$_{t,i',CP}$の係数としてｓ$_i^{CP}$ｖ$_{i,i',CP}$を設定して要素ｃ$_i^{CP}$を生成するＣＰ暗号化データ生成部と

を備え、

前記復号装置は、

前記主暗号化データ生成部が生成した要素ｃ$_0$と、前記ＫＰ暗号化データ生成部が生成した要素ｃ$_t^{KP}$と、前記ＣＰ暗号化データ生成部が生成した要素ｃ$_i^{CP}$と、前記属性集合Γ^{KP}と、前記変数ρ^{CP}（ｉ）とを含む暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$を取得するデータ取得部と、

前記主復号鍵生成部が生成した要素ｋ*$_0$と、前記ＫＰ復号鍵生成部が生成

した要素$k*_i^{KP}$と、前記ＣＰ復号鍵生成部が生成した要素$k*_t^{CP}$と、前記変数ρ^{KP}（ｉ）と、前記属性集合Γ^{CP}とを含む復号鍵$sk_{(SKP,\ \Gamma CP)}$を取得する復号鍵取得部と、

前記データ取得部が取得した暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれる属性集合Γ^{KP}と、前記復号鍵取得部が取得した復号鍵$sk_{(SKP,\ \Gamma CP)}$に含まれる変数ρ^{KP}（ｉ）とに基づき、ｉ＝１，．．．，L^{KP}の各整数ｉのうち、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$v\vec{}_i^{KP}$）であり、かつ、その組の$v\vec{}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$x\vec{}_t^{KP}$との内積が０となるｉと、変数ρ^{KP}（ｉ）が否定形の組￢（ｔ，$v\vec{}_i^{KP}$）であり、かつ、その組の$v\vec{}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$x\vec{}_t^{KP}$との内積が０とならないｉとの集合I^{KP}を特定するとともに、特定した集合I^{KP}に含まれるｉについて、$\alpha_i^{KP}M_i^{KP}$を合計した場合に前記$h\rightarrow^{KP}$となる補完係数α_i^{KP}を計算するＫＰ補完係数計算部と、

前記暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれるｉ＝１，．．．，L^{CP}の各整数ｉについての変数ρ^{CP}（ｉ）と、前記復号鍵$sk_{(SKP,\ \Gamma CP)}$に含まれる属性集合Γ^{CP}とに基づき、ｉ＝１，．．．，L^{CP}の各整数ｉのうち、変数ρ^{CP}（ｉ）が肯定形の組（ｔ，$v\vec{}_i^{CP}$）であり、かつ、その組の$v\vec{}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$x\vec{}_t^{CP}$との内積が０となるｉと、変数ρ^{CP}（ｉ）が否定形の組￢（ｔ，$v\vec{}_i^{CP}$）であり、かつ、その組の$v\vec{}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$x\vec{}_t^{CP}$との内積が０とならないｉとの集合I^{CP}を特定するとともに、特定した集合I^{CP}に含まれるｉについて、$\alpha_i^{CP}M_i^{CP}$を合計した場合に前記$h\rightarrow^{CP}$となる補完係数α_i^{CP}を計算するＣＰ補完係数計算部と、

前記暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれる要素c_0と要素c_t^{KP}と要素c_i^{CP}と、前記復号鍵$sk_{(SKP,\ \Gamma CP)}$に含まれる要素$k*_0$と要素$k*_i^{KP}$と要素$k*_t^{CP}$とについて、前記ＫＰ補完係数計算部が特定した集合I^{KP}と、前記ＫＰ補完係数計算部が計算した補完係数α_i^{KP}と、前記ＣＰ補完係数計算部が特定した集合I^{CP}と、前記ＣＰ補完係数計算部が計算した補完係数α_i^{CP}とに基

づき、数１に示すペアリング演算を行い値Ｋを計算するペアリング演算部とを備えることを特徴とする。

[数1]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_i^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_i^{CP})}$$

発明の効果

[0006] この発明に係る暗号処理システムは、復号鍵と暗号文との両方にアクセスストラクチャが埋め込まれており、多機能な暗号機能を実現している。

図面の簡単な説明

[0007] [図1]行列Ｍ＾の説明図。

[図2]行列M_{δ}の説明図。

[図3]s_0の説明図。

[図4]$s^{\rightarrow T}$の説明図。

[図5]Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式を実行する暗号処理システム１０の構成図。

[図6]鍵生成装置１００の機能を示す機能ブロック図。

[図7]暗号化装置２００の機能を示す機能ブロック図。

[図8]復号装置３００の機能を示す機能ブロック図。

[図9]Ｓｅｔｕｐアルゴリズムの処理を示すフローチャート。

[図10]ＫｅｙＧｅｎアルゴリズムの処理を示すフローチャート。

[図11]Ｅｎｃアルゴリズムの処理を示すフローチャート。

[図12]Ｄｅｃアルゴリズムの処理を示すフローチャート。

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

発明を実施するための形態

[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。つまり、処理装置、記憶装置、通信装置、入力装置はハードウェアである。

[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、

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

を示す。

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

[数107]

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

[数108]

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

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

[数109]

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

X^Tは、行列Xの転置行列を表す。

数１１０に示す基底Ｂと基底Ｂ*とに対して、数１１１である。

[数110]

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

[数111]

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

$\vec{e}_{t,j}^{KP}$, $\vec{e}_{t,j}^{CP}$は、それぞれ数１１２に示す正規基底ベクトルを示す。

[数112]

$$\vec{e}_{t,j}^{KP} : (\overbrace{0\cdots0}^{j-1}, 1, \overbrace{0\cdots0}^{n_t-j}) \in \mathbb{F}_q^{n_t^{KP}} \quad \text{for } j = 1,...,n_t^{KP},$$

$$\vec{e}_{t,j}^{CP} : (\overbrace{0\cdots0}^{j-1}, 1, \overbrace{0\cdots0}^{n_t-j}) \in \mathbb{F}_q^{n_t^{CP}} \quad \text{for } j = 1,...,n_t^{CP}$$

[0010] また、以下の説明において、F_q^{ntCP}におけるｎｔＣＰはn_t^{CP}のことである。

同様に、復号鍵$sk_{(SKP,\Gamma CP)}$におけるＳＫＰはS^{KP}のことであり、ＣＰはΓ^{CP}のことである。暗号化データ$ct_{(\Gamma KP, SCP)}$におけるΓＫＰはΓ^{KP}のことであり、ＳＣＰはS^{CP}のことである。

同様に、$param_{V0}$におけるＶ０はV_0のことである。$param_{VtKP}$におけるＶｔＫＰはV_t^{KP}のことである。$param_{VtCP}$におけるＶｔＣＰ

はV_t^{CP}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、鍵生成処理、暗号化処理、復号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、「関数型暗号（Ｆｕｎｃｔｉｏｎａｌ　Ｅｎｃｒｙｐｔｉｏｎ）方式」を実現する基礎となる概念と、関数型暗号の構成について説明する。

第１に、関数型暗号について簡単に説明する。

第２に、関数型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３に、関数型暗号を実現するための概念を説明する。ここでは、「スパンプログラム（Ｓｐａｎ　Ｐｒｏｇｒａｍ）」、「属性ベクトルの内積とアクセスストラクチャ」、「秘密分散方式（秘密共有方式）」について説明する。

第４に、この実施の形態に係る「関数型暗号方式」を説明する。この実施の形態では、「Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号（Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ　Ｆｕｎｃｔｉｏｎａｌ　Ｅｎｃｒｙｐｔｉｏｎ，ＵＰ－ＦＥ）方式」について説明する。そこで、まず、「Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式」の基本構成について説明する。次に、この「Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式」を実現する「暗号処理システム１０」の基本構成について説明する。そして、この実施の形態に係る「Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式」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．関数型暗号方式＞

関数型暗号方式は、暗号化鍵（ｅｎｃｒｙｐｔｉｏｎ－ｋｅｙ，ｅｋ）と、復号鍵（ｄｅｃｒｙｐｔｉｏｎ－ｋｅｙ，ｄｋ）との間の関係をより高度化し、より柔軟にした暗号方式である。

関数型暗号方式において、暗号化鍵と復号鍵とは、それぞれ、属性ｘと属性ｖとが設定されている。そして、関係Ｒに対してＲ（ｘ，ｖ）が成立する場合に限り、復号鍵dk_v：＝（ｄｋ，ｖ）は暗号化鍵ek_x：＝（ｅｋ，ｘ）で暗号化された暗号文を復号することができる。

関数型暗号方式には、データベースのアクセスコントロール、メールサービス、コンテンツ配布等の様々なアプリケーションが存在する（非特許文献２，７，９，１６，１９，２５－２８，３０参照）。

[0014] Ｒが等号関係である場合、つまり、ｘ＝ｖである場合に限りＲ（ｘ，ｖ）が成立する場合、関数型暗号方式はＩＤベース暗号方式である。

[0015] ＩＤベース暗号方式よりも一般化された関数型暗号方式として、属性ベース暗号方式がある。

属性ベース暗号方式では、暗号化鍵と復号鍵とに設定される属性が属性の組である。例えば、暗号化鍵と復号鍵とに設定される属性が、それぞれ、Ｘ：＝（x_1，．．．，x_d）と、Ｖ：＝（v_1，．．．，v_d）とである。

そして、属性のコンポーネントについて、コンポーネント毎の等号関係（例えば、$\{x_t = v_t\}_{t\in\{1,\ldots,d\}}$）がアクセスストラクチャＳに入力される。そして、アクセスストラクチャＳが入力を受理した場合にのみ、Ｒ（Ｘ，Ｖ）が成立する。つまり、暗号化鍵で暗号化された暗号文を復号鍵で復号することができる。

アクセスストラクチャＳが復号鍵dk_Vに埋め込まれている場合、属性ベース暗号（ＡＢＥ）方式は、Ｋｅｙ－Ｐｏｌｉｃｙ　ＡＢＥ（ＫＰ－ＡＢＥ）と呼ばれる。一方、アクセスストラクチャＳが暗号文に埋め込まれている場合、属性ベース暗号（ＡＢＥ）方式は、Ｃｉｐｈｅｒｔｅｘｔ－Ｐｏｌｉｃ

ｙ　ＡＢＥ（ＣＰ－ＡＢＥ）と呼ばれる。そして、アクセスストラクチャＳが復号鍵dk_Vと暗号文との両方に埋め込まれている場合、属性ベース暗号（ＡＢＥ）方式は、Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ　ＡＢＥ（ＵＰ－ＡＢＥ）と呼ばれる。

[0016] 非特許文献１９に記載された内積述語暗号（Ｉｎｎｅｒ－Ｐｒｏｄｕｃｔ Ｅｎｃｒｙｐｔｉｏｎ，ＩＰＥ）も関数型暗号の１つのクラスである。ここでは、暗号化鍵と復号鍵とに設定される属性がぞれぞれ体又は環上のベクトルである。例えば、$\vec{x} := (x_1, \ldots, x_n) \in F_q^n$と$\vec{v} := (v_1, \ldots, v_n) \in F_q^n$とがそれぞれ暗号化鍵と復号鍵とに設定される。そして、$\vec{x} \cdot \vec{v} = 0$である場合に限り、$R(\vec{x}, \vec{v})$が成立する。

[0017] ＜第２．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１１３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113]

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

[0018] 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１１４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１１５に示す通りである。

[数114]

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

[数115]

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

[0019] 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１１６によって定義される。

[数116]

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

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）$^{δ_{ｉ,ｊ}}$である。ここで、ｉ＝ｊであれば、$δ_{ｉ,ｊ}$＝１であり、ｉ≠ｊであれば、$δ_{ｉ,ｊ}$＝０である。また、ｅ（ｇ，ｇ）≠１∈$Ｇ_{Ｔ}$である。

[0020] 演算（２）：ディストーション写像

数１１７に示す空間Ｖにおける線形変換$φ_{ｉ,ｊ}$は、数１１８を行うことができる。

[数117]

$\phi_{i,j}(a_j) = a_i$であり、

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

[数118]

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

ここで、

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

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。

[0021] 以下の説明において、数１１９を、1^{λ}（$\lambda \in$自然数）、N∈自然数、双線形ペアリング群のパラメータ$param_G := (q, G, G_T, g, e)$の値を入力として、セキュリティパラメータが$\lambda$であり、N次元の空間Vとする双対ペアリングベクトル空間のパラメータ$param_V := (q, V, G_T, A, e)$の値を出力するアルゴリズムとする。

[数119]

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

[0022] 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。

[0023] ＜第３．関数型暗号を実現するための概念＞

＜第３－１．スパンプログラム＞

図１は、行列Ｍ＾の説明図である。

｛ｐ$_1$，．．．，ｐ$_n$｝を変数の集合とする。Ｍ＾：＝（Ｍ，ρ）は、ラベル付けされた行列である。ここで、行列Ｍは、Ｆ$_q$上の（Ｌ行×ｒ列）の行列である。また、ρは、行列Ｍの各列に付されたラベルであり、｛ｐ$_1$，．．．，ｐ$_n$，￢ｐ$_1$，．．．，￢ｐ$_n$｝のいずれか１つのリテラルへ対応付けられる。なお、Ｍの全ての行に付されたラベルρ$_i$（ｉ＝１，．．．，Ｌ）がいずれか１つのリテラルへ対応付けられる。つまり、ρ：｛１，．．．，Ｌ｝→｛ｐ$_1$，．．．，ｐ$_n$，￢ｐ$_1$，．．．，￢ｐ$_n$｝である。

[0024] 全ての入力列δ∈｛０，１｝^{n}に対して、行列Ｍの部分行列Ｍ$_δ$は定義される。行列Ｍ$_δ$は、入力列δによってラベルρに値“１”が対応付けられた行列Ｍの行から構成される部分行列である。つまり、行列Ｍ$_δ$は、δ$_i$＝１であるようなｐ$_i$に対応付けられた行列Ｍの行と、δ$_i$＝０であるような￢ｐ$_i$に対応付けられた行列Ｍの行とからなる部分行列である。

図２は、行列Ｍ$_δ$の説明図である。なお、図２では、ｎ＝７，Ｌ＝６，ｒ＝５としている。つまり、変数の集合は、｛ｐ$_1$，．．．，ｐ$_7$｝であり、行列Ｍは（６行×５列）の行列である。また、図２において、ラベルρは、ρ$_1$が￢ｐ$_2$に、ρ$_2$がｐ$_1$に、ρ$_3$がｐ$_4$に、ρ$_4$が￢ｐ$_5$に、ρ$_5$が￢ｐ$_3$に、ρ$_6$がｐ$_5$にそれぞれ対応付けられているとする。

ここで、入力列δ∈｛０，１｝^{7}が、δ$_1$＝１，δ$_2$＝０，δ$_3$＝１，δ$_4$＝０，δ$_5$＝０，δ$_6$＝１，δ$_7$＝１であるとする。この場合、破線で囲んだリテラル（ｐ$_1$，ｐ$_3$，ｐ$_6$，ｐ$_7$，￢ｐ$_2$，￢ｐ$_4$，￢ｐ$_5$）に対応付けられている行列Ｍの行からなる部分行列が行列Ｍ$_δ$である。つまり、行列Ｍの１行目（Ｍ$_1$），２行目（Ｍ$_2$），４行目（Ｍ$_4$）からなる部分行列が行列Ｍ$_δ$である。

[0025] 言い替えると、写像γ：｛１，．．．，Ｌ｝→｛０，１｝が、［ρ（ｊ）＝ｐ$_i$］∧［δ$_i$＝１］又は［ρ（ｊ）＝￢ｐ$_i$］∧［δ$_i$＝０］である場合、γ（ｊ）＝１であり、他の場合、γ（ｊ）＝０であるとする。この場合に、Ｍ$_δ$：＝（Ｍ$_j$）$_{γ(j)=1}$である。ここで、Ｍ$_j$は、行列Ｍのｊ番目の行である。

つまり、図２では、写像γ（ｊ）＝１（ｊ＝１，２，４）であり、写像γ（ｊ）＝０（ｊ＝３，５，６）である。したがって、$(M_j)_{\gamma(j)=1}$は、M_1，M_2，M_4であり、行列M_δである。

すなわち、写像γ（ｊ）の値が“０”であるか“１”であるかによって、行列Ｍのｊ番目の行が行列M_δに含まれるか否かが決定される。

[0026] $1^{\rightarrow} \in span\langle M_\delta \rangle$である場合に限り、スパンプログラムＭ＾は入力列δを受理し、他の場合には入力列δを拒絶する。つまり、入力列δによって行列Ｍ＾から得られる行列M_δの行を線形結合して$1^{\rightarrow}$が得られる場合に限り、スパンプログラムＭ＾は入力列δを受理する。なお、$1^{\rightarrow}$とは、各要素が値“１”である行ベクトルである。

例えば、図２の例であれば、行列Ｍの１，２，４行目からなる行列M_δの各行を線形結合して$1^{\rightarrow}$が得られる場合に限り、スパンプログラムＭ＾は入力列δを受理する。つまり、$\alpha_1(M_1)+\alpha_2(M_2)+\alpha_4(M_4)=1^{\rightarrow}$となる$\alpha_1$，$\alpha_2$，$\alpha_4$が存在する場合には、スパンプログラムＭ＾は入力列δを受理する。

[0027] ここで、ラベルρが正のリテラル｛p_1，．．．，p_n｝にのみ対応付けられている場合、スパンプログラムはモノトーンと呼ばれる。一方、ラベルρがリテラル｛p_1，．．．，p_n，$\neg p_1$，．．．，$\neg p_n$｝に対応付けられている場合、スパンプログラムはノンモノトーンと呼ばれる。ここでは、スパンプログラムはノンモノトーンとする。そして、ノンモノトーンスパンプログラムを用いて、アクセスストラクチャ（ノンモノトーンアクセスストラクチャ）を構成する。アクセスストラクチャとは、簡単に言うと暗号へのアクセス制御を行うものである。つまり、暗号文を復号できるか否かの制御を行うものである。

詳しくは後述するが、スパンプログラムがモノトーンではなく、ノンモノトーンであることにより、スパンプログラムを利用して構成する関数型暗号方式の利用範囲が広がる。

[0028] ＜第３－２．属性ベクトルの内積とアクセスストラクチャ＞

ここでは、属性ベクトルの内積を用いて上述した写像γ（ｊ）を計算する。つまり、属性ベクトルの内積を用いて、行列Ｍのどの行を行列M_{δ}に含めるかを決定する。

[0029] U_t（ｔ＝１，．．．，ｄであり$U_t \subset \{0, 1\}^*$）は、部分全集合（ｓｕｂ－ｕｎｉｖｅｒｓｅ）であり、属性の集合である。そして、U_tは、それぞれ部分全集合の識別情報（ｔ）と、n_t次元ベクトル（$v^{\rightarrow}$）とを含む。つまり、U_tは、（ｔ，$v^{\rightarrow}$）である。ここで、$t \in \{1, \ldots, d\}$であり、$v^{\rightarrow} \in F_q^{n_t}$である。

[0030] U_t：＝（ｔ，$v^{\rightarrow}$）をスパンプログラム$M\hat{}$：＝（Ｍ，ρ）における変数ｐとする。つまり、ｐ：＝（ｔ，$v^{\rightarrow}$）である。そして、変数（ｐ：＝（ｔ，$v^{\rightarrow}$），（ｔ’，$v'^{\rightarrow}$），．．．）としたスパンプログラム$M\hat{}$：＝（Ｍ，ρ）をアクセスストラクチャＳとする。

つまり、アクセスストラクチャＳ：＝（Ｍ，ρ）であり、ρ：｛１，．．．，Ｌ｝→｛（ｔ，$v^{\rightarrow}$），（ｔ’，$v'^{\rightarrow}$），．．．，¬（ｔ，$v^{\rightarrow}$），¬（ｔ’，$v'^{\rightarrow}$），．．．｝である。

[0031] 次に、Γを属性の集合とする。つまり、Γ：＝｛（ｔ，$x^{\rightarrow}_t$）｜$x^{\rightarrow}_t \in F_q^{n_t}$，$1 \leqq t \leqq d$｝である。

アクセスストラクチャＳにΓが与えられた場合、スパンプログラム$M\hat{}$：＝（Ｍ，ρ）に対する写像γ：｛１，．．．，Ｌ｝→｛０，１｝は、以下のように定義される。ｉ＝１，．．．，Ｌの各整数ｉについて、［ρ（ｉ）＝（ｔ，$v^{\rightarrow}_i$）］∧［（ｔ，$x^{\rightarrow}_t$）∈Γ］∧［$v^{\rightarrow}_i \cdot x^{\rightarrow}_t = 0$］、又は、［ρ（ｉ）＝¬（ｔ，$v^{\rightarrow}_i$）］∧［（ｔ，$x^{\rightarrow}_t$）∈Γ］∧［$v^{\rightarrow}_i \cdot x^{\rightarrow}_t \neq 0$］である場合、γ（ｊ）＝１であり、他の場合、γ（ｊ）＝０とする。

つまり、属性ベクトル$v^{\rightarrow}$と$x^{\rightarrow}$との内積に基づき、写像γが計算される。そして、上述したように、写像γにより、行列Ｍのどの行を行列M_{δ}に含めるかが決定される。すなわち、属性ベクトル$v^{\rightarrow}$と$x^{\rightarrow}$との内積により、行列Ｍのどの行を行列M_{δ}に含めるかが決定され、$1^{\rightarrow} \in span\langle (M_i)_{\gamma(i)=1} \rangle$である場合に限り、アクセスストラクチャＳ：＝（Ｍ，ρ）はΓを受理す

る。

[0032] ＜第３－３．秘密分散方式＞

アクセスストラクチャＳ：＝（Ｍ，ρ）に対する秘密分散方式について説明する。

なお、秘密分散方式とは、秘密情報を分散させ、意味のない分散情報にすることである。例えば、秘密情報ｓを１０個に分散させ、１０個の分散情報を生成する。ここで、１０個の分散情報それぞれは、秘密情報ｓの情報を有していない。したがって、ある１個の分散情報を手に入れても秘密情報ｓに関して何ら情報を得ることはできない。一方、１０個の分散情報を全て手に入れれば、秘密情報ｓを復元できる。

また、１０個の分散情報を全て手に入れなくても、一部だけ（例えば、８個）手に入れれば秘密情報ｓを復元できる秘密分散方式もある。このように、１０個の分散情報のうち８個で秘密情報ｓを復元できる場合を、８－ｏｕｔ－ｏｆ－１０と呼ぶ。つまり、ｎ個の分散情報のうちｔ個で秘密情報ｓを復元できる場合を、ｔ－ｏｕｔ－ｏｆ－ｎと呼ぶ。このｔを閾値と呼ぶ。

また、d_1，．．．，d_{10}の１０個の分散情報を生成した場合に、d_1，．．．，d_8までの８個の分散情報であれば秘密情報ｓを復元できるが、d_3，．．．，d_{10}までの８個の分散情報であれば秘密情報ｓを復元できないというような秘密分散方式もある。つまり、手に入れた分散情報の数だけでなく、分散情報の組合せに応じて秘密情報ｓを復元できるか否かを制御する秘密分散方式もある。

[0033] 図３は、s_0の説明図である。図４は、$s^{\rightarrow T}$の説明図である。

行列Ｍを（Ｌ行×ｒ列）の行列とする。$f^{\rightarrow T}$を数１２０に示す列ベクトルとする。

[数120]

$$\vec{f}^{\mathrm{T}} := (f_1, \ldots f_r)^T \xleftarrow{U} \mathbb{F}_q^r$$

数１２１に示すs_0を共有される秘密情報とする。

[数121]

$$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}} := \sum_{k=1}^{r} f_k$$

また、数１２２に示すｓ$^{\rightarrow \mathrm{T}}$をｓ$_0$のＬ個の分散情報のベクトルとする。

[数122]

$$\vec{s}^{\mathrm{T}} := (s_1, \ldots s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$$

そして、分散情報ｓ$_i$をρ（ｉ）に属するものとする。

[0034] アクセスストラクチャＳ：＝（Ｍ，ρ）がΓを受理する場合、つまりγ：｛１，．．．，Ｌ｝→｛０，１｝について$1^{\rightarrow} \in \mathrm{span}\langle (M_i)_{\gamma(i)=1} \rangle$である場合、Ｉ⊆｛ｉ∈｛１，．．．，Ｌ｝｜γ（ｉ）−＝１｝である定数｛$\alpha_i \in F_q$｜ｉ∈Ｉ｝が存在する。

これは、図２の例で、$\alpha_1 (M_1) + \alpha_2 (M_2) + \alpha_4 (M_4) = 1^{\rightarrow}$となる$\alpha_1$，$\alpha_2$，$\alpha_4$が存在する場合には、スパンプログラムＭ＾は入力列δを受理すると説明したことからも明らかである。つまり、$\alpha_1 (M_1) + \alpha_2 (M_2) + \alpha_4 (M_4) = 1^{\rightarrow}$となる$\alpha_1$，$\alpha_2$，$\alpha_4$が存在する場合には、スパンプログラムＭ＾が入力列δを受理するのであれば、$\alpha_1 (M_1) + \alpha_2 (M_2) + \alpha_4 (M_4) = 1^{\rightarrow}$となる$\alpha_1$，$\alpha_2$，$\alpha_4$が存在する。

そして、数１２３である。

[数123]

$$\sum_{i \in I} \alpha_i s_i := s_0$$

なお、定数｛α_i｝は、行列Ｍのサイズにおける多項式時間で計算可能である。

[0035] この実施の形態及び以下の実施の形態に係る関数型暗号方式は、上述したように、スパンプログラムに内積述語と秘密分散方式とを適用してアクセスストラクチャを構成する。そのため、スパンプログラムにおける行列Ｍや、

内積述語における属性情報ｘ及び属性情報ｖ（述語情報）を設計するにより、アクセス制御を自由に設計することができる。つまり、非常に高い自由度でアクセス制御の設計を行うことができる。なお、行列Ｍの設計は、秘密分散方式の閾値等の条件設計に相当する。

例えば、上述した属性ベース暗号方式は、この実施の形態及び以下の実施の形態に係る関数型暗号方式におけるアクセスストラクチャにおいて、内積述語の設計をある条件に限定した場合に相当する。つまり、この実施の形態及び以下の実施の形態に係る関数型暗号方式におけるアクセスストラクチャに比べ、属性ベース暗号方式におけるアクセスストラクチャは、内積述語における属性情報ｘ及び属性情報ｖ（述語情報）を設計の自由度がない分、アクセス制御の設計の自由度が低い。なお、具体的には、属性ベース暗号方式は、属性情報 $\{\vec{x}_t\}_{t\in\{1,\ldots,d\}}$ と $\{\vec{v}_t\}_{t\in\{1,\ldots,d\}}$ とを、等号関係に対する２次元ベクトル、例えば $\vec{x}_t := (1, x_t)$ と $\vec{v}_t := (v_t, -1)$ とに限定した場合に相当する。

また、上述した内積述語暗号方式は、この実施の形態及び以下の実施の形態に係る関数型暗号方式におけるアクセスストラクチャにおいて、スパンプログラムにおける行列Ｍの設計をある条件に限定した場合に相当する。つまり、この実施の形態及び以下の実施の形態に係る関数型暗号方式におけるアクセスストラクチャに比べ、内積述語暗号方式におけるアクセスストラクチャは、スパンプログラムにおける行列Ｍの設計の自由度がない分、アクセス制御の設計の自由度が低い。なお、具体的には、内積述語暗号方式は、秘密分散方式を１－ｏｕｔ－ｏｆ－１（あるいは、ｄ－ｏｕｔ－ｏｆ－ｄ）に限定した場合である。

[0036] 特に、この実施の形態及び以下の実施の形態に係る関数型暗号方式におけるアクセスストラクチャは、ノンモノトーンスパンプログラムを用いたノンモノトーンアクセスストラクチャを構成する。そのため、アクセス制御の設計の自由度がより高くなる。

具体的には、ノンモノトーンスパンプログラムには、否定形のリテラル（

¬ｐ）を含むため、否定形の条件を設定できる。例えば、第１会社には、Ａ部とＢ部とＣ部とＤ部との４つの部署があったとする。ここで、第１会社のＢ部以外の部署の属するユーザにのみアクセス可能（復号可能）というアクセス制御をしたいとする。この場合に、否定形の条件の設定ができないとすると、「第１会社のＡ部とＣ部とＤ部とのいずれかに属すること」という条件を設定する必要がある。一方、否定形の条件の設定ができるとすると、「第１会社の社員であって、Ｂ部以外に属すること」という条件を設定することができる。つまり、否定形の条件が設定できることで、自然な条件設定が可能となる。なお、ここでは部署の数が少ないが、部署の数が多い場合等は非常に有効であることが分かる。

[0037] ＜第４．関数型暗号方式の基本構成＞

＜第４－１．Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式の基本構成＞

Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式の構成を簡単に説明する。なお、Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙとは、復号鍵及び暗号文にＰｏｌｉｃｙが埋め込まれること、つまりアクセスストラクチャが埋め込まれることを意味する。

Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式は、Ｓｅｔｕｐ、ＫｅｙＧｅｎ、Ｅｎｃ、Ｄｅｃの４つのアルゴリズムを備える。

（Ｓｅｔｕｐ）

Ｓｅｔｕｐアルゴリズムは、セキュリティパラメータλと、属性のフォーマット$\vec{n}:=((d^{KP};n_t^{KP},u_t^{KP},w_t^{KP},z_t^{KP}(t=1,...,d^{KP})),(d^{CP};n_t^{CP},u_t^{CP},w_t^{CP},z_t^{CP}(t=1,...,d^{CP})))$とが入力され、公開パラメータｐｋと、マスター鍵ｓｋとを出力する確率的アルゴリズムである。

（ＫｅｙＧｅｎ）

ＫｅｙＧｅｎアルゴリズムは、アクセスストラクチャ$S^{KP}:=(M^{KP},\rho^{KP})$と、属性の集合である$\Gamma^{CP}:=\{(t,\vec{x}_t^{CP})\mid \vec{x}_t^{CP}\in F_q^{nt^{CP}}\setminus\{\vec{0}\},1\leqq t\leqq d^{CP}\}$と、公開パラメータｐｋと、マスター鍵ｓｋとを入力

として、復号鍵ｓｋ$_{(SKP,\Gamma CP)}$を出力する確率的アルゴリズムである。

（Ｅｎｃ）

Ｅｎｃアルゴリズムは、メッセージｍと、属性の集合であるΓ^{KP}：＝｛（ｔ，$\vec{x}_t^{KP}$）｜$\vec{x}_t^{KP}\in F_q^{ntKP}\setminus\{\vec{0}\}$，１≦ｔ≦$d^{KP}$｝と、アクセスストラクチャ$S^{CP}$：＝（$M^{CP}$，$\rho^{CP}$）と、公開パラメータｐｋとを入力として、暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$を出力する確率的アルゴリズムである。

（Ｄｅｃ）

Ｄｅｃアルゴリズムは、属性の集合及びアクセスストラクチャ（Γ^{KP}，S^{CP}）の下で暗号化された暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$と、アクセスストラクチャ及び属性の集合（S^{KP}，Γ^{CP}）に対する復号鍵ｓｋ$_{(SKP,\Gamma CP)}$と、公開パラメータｐｋとを入力として、メッセージｍ（平文情報）、又は、識別情報⊥を出力するアルゴリズムである。

[0038] Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式は、数１２４に示す全ての公開パラメータｐｋ及びマスター鍵ｓｋと、全てのアクセスストラクチャS^{KP}と、全ての属性の集合Γ^{CP}と、数１２５に示す全ての復号鍵ｓｋ$_{(SKP,\Gamma CP)}$と、全てのメッセージｍと、全ての属性の集合Γ^{KP}と、全てのアクセスストラクチャS^{CP}と、数１２６に示す全ての暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$とに対して、アクセスストラクチャS^{KP}が属性の集合Γ^{KP}を受理し、かつ、アクセスストラクチャS^{CP}が属性の集合Γ^{CP}を受理する場合、圧倒的な確率でｍ＝Ｄｅｃ（ｐｋ，ｓｋ$_{(SKP,\Gamma CP)}$，ｃｔ$_{(\Gamma KP,\ SCP)}$）である。つまり、公開パラメータｐｋと、復号鍵ｓｋ$_{(SKP,\Gamma CP)}$と、暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$とを入力としてＤｅｃアルゴリズムを実行することで、メッセージｍを得ることができる。

[数124]

$$(\mathrm{pk},\mathrm{sk})\xleftarrow{R}\mathrm{Setup}(1^{\lambda},\vec{n})$$

[数125]

$$\mathrm{sk}_{(\mathbb{S}^{KP},\Gamma^{CP})} \xleftarrow{R} \mathrm{KeyGen}(\mathrm{pk},\mathrm{sk},\mathbb{S}^{KP},\Gamma^{CP})$$

[数126]

$$\mathrm{ct}_{(\Gamma^{KP},\mathbb{S}^{CP})} \xleftarrow{R} \mathrm{Enc}(\mathrm{pk},m,\Gamma^{KP},\mathbb{S}^{CP})$$

[0039] ＜第４－２．暗号処理システム１０＞

上述したＵｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型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５は、Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式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を備える。

鍵生成装置１００は、セキュリティパラメータλと、属性のフォーマット$\vec{n}:=((d^{KP};n_t^{KP},u_t^{KP},w_t^{KP},z_t^{KP}(t=1,...,d^{KP})),(d^{CP};n_t^{CP},u_t^{CP},w_t^{CP},z_t^{CP}(t=1,...,d^{CP})))$とを入力としてＳｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター鍵ｓｋとを生成する。そして、鍵生成装置１００は、生成した公開パラメータｐｋを公開する。また、鍵生成装置１００は、アクセスストラクチャ$\mathbb{S}^{KP}$と、属性の集合Γ^{CP}と、公開パラメータｐｋと、マスター鍵ｓｋとを入力としてＫｅｙＧｅｎアルゴリズムを実行して、復号鍵$\mathrm{sk}_{(\mathbb{S}^{KP},\Gamma^{CP})}$を生成して復号装置３００へ秘密裡に配布する。

暗号化装置２００は、メッセージｍと、属性の集合Γ^{KP}と、アクセスストラクチャ$\mathbb{S}^{CP}$と、公開パラメータｐｋとを入力としてＥｎｃアルゴリズムを実行して、暗号化データ$\mathrm{ct}_{(\Gamma^{KP},\mathbb{S}^{CP})}$を生成する。暗号化装置２００は、生成した暗号化データ$\mathrm{ct}_{(\Gamma^{KP},\mathbb{S}^{CP})}$を復号装置３００へ送信する。

復号装置３００は、公開パラメータｐｋと、復号鍵$\mathrm{sk}_{(\mathbb{S}^{KP},\Gamma^{CP})}$と、暗号化データ$\mathrm{ct}_{(\Gamma^{KP},\mathbb{S}^{CP})}$とを入力としてＤｅｃアルゴリズムを実行して、

メッセージｍ又は識別情報Ｌを出力する。

[0040] ＜第４－３．Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式及び暗号処理システム１０の詳細＞

図６から図１２に基づき、Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号方式、及び、Ｕｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型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６は、鍵生成装置１００の機能を示す機能ブロック図である。図７は、暗号化装置２００の機能を示す機能ブロック図である。図８は、復号装置３００の機能を示す機能ブロック図である。

図９と図１０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９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１０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１１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１２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。

なお、ここでは、$x_{t,1}^{KP}:=1$，$x_{t,1}^{CP}:=1$に正規化する。なお、$x_{t,1}^{KP}$及び$x_{t,1}^{CP}$が正規化されていない場合、$(1/x_{t,1}^{KP})\cdot x_{t,1}^{KP}$、及び、$(1/x_{t,1}^{CP})\cdot x_{t,1}^{CP}$として正規化すればよい。この場合、$x_{t,i}^{KP}$及び$x_{t,i}^{CP}$は０でないものとする。

[0041] 鍵生成装置１００の機能と動作とについて説明する。

図６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を備える。

また、情報入力部１３０は、ＫＰ情報入力部１３１（第１ＫＰ情報入力部）、ＣＰ情報入力部１３２（第１ＣＰ情報入力部）を備える。また、復号鍵生成部１４０は、ｆベクトル生成部１４１、ｓベクトル生成部１４２、乱数生成部１４３、主復号鍵生成部１４４、ＫＰ復号鍵生成部１４５、ＣＰ復号

鍵生成部１４６を備える。

[0042] まず、図９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１２７を計算して、$param_{n\to}$と、基底B_0及び基底B^*_0と、ｔ＝１，．．．，d^{KP}の各整数ｔについて基底B_t^{KP}及び基底$B^*_t{}^{KP}$と、ｔ＝１，．．．，d^{CP}の各整数ｔについて基底B_t^{CP}及び基底$B^*_t{}^{CP}$とをランダムに生成する。

[数127]

$$\mathcal{G}_{\mathsf{ob}}{}^{\mathsf{up}}(1^{\lambda},\vec{n}:=((d^{\mathsf{KP}};n_t^{\mathsf{KP}},u_t^{\mathsf{KP}},w_t^{\mathsf{KP}},z_t^{\mathsf{KP}}\left(t=1,...,d^{\mathsf{KP}}\right)),$$
$$(d^{\mathsf{CP}};n_t^{\mathsf{CP}},u_t^{\mathsf{CP}},w_t^{\mathsf{CP}},z_t^{\mathsf{CP}}\left(t=1,...,d^{\mathsf{CP}}\right))):$$
$$\mathsf{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{\mathsf{R}}\mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),\quad \psi\xleftarrow{\mathsf{U}}\mathbb{F}_q^{\times},$$
$$N_0:=2+u_0+1+w_0+z_0,$$
$$N_t^{\mathsf{KP}}:=n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}}\ \text{ for } t=1,\ldots,d^{\mathsf{KP}},$$
$$N_t^{\mathsf{CP}}:=n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}}\ \text{ for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\mathsf{param}_{\mathbb{V}_0}:=(q,\mathbb{V}_0,\mathbb{G}_T,\mathbb{A}_0,e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_0,\mathsf{param}_{\mathbb{G}}),$$
$$X_0:=(\chi_{0,i,j})_{i,j}\xleftarrow{\mathsf{U}}GL(N_0,\mathbb{F}_q),\quad (\nu_{0,i,j})_{i,j}:=\psi\cdot(X_0^{\mathrm{T}})^{-1},$$
$$b_{0,i}:=(\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0:=(b_{0,1},\ldots,b_{0,N_0}),$$
$$b_{0,i}^*:=(\nu_{0,i,1},\ldots,\nu_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0^*:=(b_{0,i}^*,\ldots,b_{0,N_0}^*),$$
$$\text{for } t=1,\ldots,d^{\mathsf{KP}},$$
$$\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}:=(q,\mathbb{V}_t^{\mathsf{KP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{KP}},e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{KP}},\mathsf{param}_{\mathbb{G}}),$$
$$X_t^{\mathsf{KP}}:=(\chi_{t,i,j}^{\mathsf{KP}})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t^{\mathsf{KP}},\mathbb{F}_q),\quad (\nu_{t,i,j}^{\mathsf{KP}})_{i,j}:=\psi\cdot((X_t^{\mathsf{KP}})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{\mathsf{KP}}:=(\chi_{t,i,1}^{\mathsf{KP}},\ldots,\chi_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{\mathsf{KP}}:=(b_{t,1}^{\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{\mathsf{KP}}),$$
$$b_{t,i}^{*\mathsf{KP}}:=(\nu_{t,i,1}^{\mathsf{KP}},\ldots,\nu_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{*\mathsf{KP}}:=(b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$
$$\text{for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}:=(q,\mathbb{V}_t^{\mathsf{CP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{CP}},e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{CP}},\mathsf{param}_{\mathbb{G}}),$$
$$X_t^{\mathsf{CP}}:=(\chi_{t,i,j}^{\mathsf{CP}})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t^{\mathsf{CP}},\mathbb{F}_q),\quad (\nu_{t,i,j}^{\mathsf{CP}})_{i,j}:=\psi\cdot((X_t^{\mathsf{CP}})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{\mathsf{CP}}:=(\chi_{t,i,1}^{\mathsf{CP}},\ldots,\chi_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{\mathsf{CP}}:=(b_{t,1}^{\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{\mathsf{CP}}),$$
$$b_{t,i}^{*\mathsf{CP}}:=(\nu_{t,i,1}^{\mathsf{CP}},\ldots,\nu_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{*\mathsf{CP}}:=(b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$
$$g_T:=e(g,g)^{\psi},$$
$$\mathsf{param}_{\vec{n}}:=(\mathsf{param}_{\mathbb{V}_0},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}\}_{t=1,\ldots,d^{\mathsf{CP}}},g_T)$$
$$\text{return } (\mathsf{param}_{\vec{n}},\{\mathbb{B}_0,\mathbb{B}_0^*\},\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}).$$

[0043] つまり、マスター鍵生成部１１０は以下の処理を実行する。

まず、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$\vec{n}:=((d^{KP};n_t^{KP},u_t^{KP},w_t^{KP},z_t^{KP}(t=1,\ldots,d^{KP})),(d^{CP};n_t^{CP},u_t^{CP},w_t^{CP}$

，z_t^{CP}（t＝1，．．．，d^{CP}））とを入力する。ここで、d^{KP}は１以上の整数であり、t＝1，．．．，d^{KP}までの各整数tについてn_t^{KP}，u_t^{KP}，w_t^{KP}，z_t^{KP}は１以上の整数である。また、d^{CP}は１以上の整数であり、t＝1，．．．，d^{CP}までの各整数tについてn_t^{CP}，u_t^{CP}，w_t^{CP}，z_t^{CP}は１以上の整数である。

[0044] 次に、マスター鍵生成部１１０は、処理装置により、数１２８を計算する。

[数128]

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

つまり、マスター鍵生成部１１０は、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、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。

[0045] 次に、マスター鍵生成部１１０は、処理装置により、数１２９を計算する。

[数129]

$$\begin{aligned}
&\psi \xleftarrow{U} \mathbb{F}_q^{\times},\\
&N_0 := 2+u_0+1+w_0+z_0,\\
&N_t^{\mathsf{KP}} := n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}} \quad \text{for } t=1,\ldots,d^{\mathsf{KP}},\\
&N_t^{\mathsf{CP}} := n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}} \quad \text{for } t=1,\ldots,d^{\mathsf{CP}}
\end{aligned}$$

つまり、マスター鍵生成部１１０は、乱数ψを生成する。また、マスター鍵生成部１１０は、N_0に２＋u_0＋１＋w_0＋z_0を設定し、t＝1，．．．，d^{KP}の各整数tについてN_t^{KP}にn_t^{KP}＋u_t^{KP}＋w_t^{KP}＋z_t^{KP}を設定し、t＝1，．．．，d^{CP}の各整数tについてN_t^{CP}にn_t^{CP}＋u_t^{CP}＋w_t^{CP}＋z_t^{CP}を設定する。ここで、u_0，w_0，z_0は１以上の整数である。

[0046] 次に、マスター鍵生成部１１０は、処理装置により、数１３０を計算する。

[数130]

$$\mathsf{param}_{\mathbb{V}_0} := (q, \mathbb{V}_0, \mathbb{G}_T, \mathbb{A}_0, e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_0, \mathsf{param}_{\mathbb{G}}),$$
$$X_0 := (\chi_{0,i,j})_{i,j} \xleftarrow{\cup} GL(N_0, \mathbb{F}_q),$$
$$(\nu_{0,i,j})_{i,j} := \psi \cdot (X_0^{\mathrm{T}})^{-1},$$
$$b_{0,i} := (\chi_{0,i,1}, \ldots, \chi_{0,i,N_0})_{\mathbb{A}_0}, \quad \mathbb{B}_0 := (b_{0,1}, \ldots, b_{0,N_0}),$$
$$b^*_{0,i} := (\nu_{0,i,1}, \ldots, \nu_{0,i,N_0})_{\mathbb{A}_0}, \quad \mathbb{B}^*_0 := (b^*_{0,i}, \ldots, b^*_{0,N_0})$$

つまり、マスター鍵生成部１１０は、入力したセキュリティパラメータλ（1^λ）と、設定したN_0と、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$param_{V0}$：＝（q，V_0，G_T，A_0，e）の値を生成する。

また、マスター鍵生成部１１０は、設定したN_0と、F_qとを入力として、線形変換X_0：＝$(\chi_{0,i,j})_{i,j}$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、$(\chi_{0,i,j})_{i,j}$は、行列$\chi_{0,i,j}$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_0である。

また、マスター鍵生成部１１０は、乱数φと線形変換X_0とに基づき、$(\nu_{0,i,j})_{i,j}$：＝φ・$(X_0{}^{T})^{-1}$を生成する。なお、$(\nu_{0,i,j})_{i,j}$も$(\chi_{0,i,j})_{i,j}$と同様に、行列$\nu_{0,i,j}$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_0である。

そして、マスター鍵生成部１１０は、線形変換X_0に基づき、標準基底A_0から基底B_0を生成する。同様に、マスター鍵生成部１１０は、$(\nu_{0,i,j})_{i,j}$に基づき、標準基底A_0から基底B^*_0を生成する。

[0047] 次に、マスター鍵生成部１１０は、処理装置により、数１３１を計算する。

[数131]

$$\begin{aligned}
&\text{for } t=1,\ldots,d^{\mathsf{KP}},\\
&\quad \mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}} := (q,\mathbb{V}_t^{\mathsf{KP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{KP}},e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{KP}},\mathsf{param}_{\mathbb{G}}),\\
&\quad X_t^{\mathsf{KP}} := (\chi_{t,i,j}^{\mathsf{KP}})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t^{\mathsf{KP}},\mathbb{F}_q),\\
&\quad (\nu_{t,i,j}^{\mathsf{KP}})_{i,j} := \psi\cdot((X_t^{\mathsf{KP}})^{\mathrm{T}})^{-1},\\
&\quad b_{t,i}^{\mathsf{KP}} := (\chi_{t,i,1}^{\mathsf{KP}},\ldots,\chi_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{\mathsf{KP}} := (b_{t,1}^{\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{\mathsf{KP}}),\\
&\quad b_{t,i}^{*\mathsf{KP}} := (\nu_{t,i,1}^{\mathsf{KP}},\ldots,\nu_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{*\mathsf{KP}} := (b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{*\mathsf{KP}})
\end{aligned}$$

つまり、マスター鍵生成部１１０は、ｔ＝１，．．．，ｄ^{KP}の各整数ｔについて以下の処理を実行する。

マスター鍵生成部１１０は、入力したセキュリティパラメータλ（１$^{\lambda}$）と、設定したＮ$_{t}^{KP}$と、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$_{VtKP}$：＝（ｑ，Ｖ$_{t}^{KP}$，Ｇ$_{T}$，Ａ$_{t}^{KP}$，ｅ）の値を生成する。

また、マスター鍵生成部１１０は、設定したＮ$_{t}^{KP}$と、Ｆ$_{q}$とを入力として、線形変換Ｘ$_{t}^{KP}$：＝（χ$_{t}^{KP}$$_{,i,j}$）$_{i,j}$をランダムに生成する。（χ$_{t}^{KP}$$_{,i,j}$）$_{i,j}$は、行列χ$_{t}^{KP}$$_{,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}^{KP}$である。

また、マスター鍵生成部１１０は、乱数φと線形変換Ｘ$_{t}^{KP}$とに基づき、（ν$_{t}^{KP}$$_{,i,j}$）$_{i,j}$：＝φ・（（Ｘ$_{t}^{KP}$）^{T}）$^{-1}$を生成する。なお、（ν$_{t}^{KP}$$_{,i,j}$）$_{i,j}$も（χ$_{t}^{KP}$$_{,i,j}$）$_{i,j}$と同様に、行列ν$_{t}^{KP}$$_{,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}^{KP}$である。

そして、マスター鍵生成部１１０は、線形変換Ｘ$_{t}^{KP}$に基づき、標準基底Ａ$_{t}^{KP}$から基底Ｂ$_{t}^{KP}$を生成する。同様に、マスター鍵生成部１１０は、（ν$_{t}^{KP}$$_{,i,j}$）$_{i,j}$に基づき、標準基底Ａ$_{t}^{KP}$から基底Ｂ＊$_{t}^{KP}$を生成する。

[0048] 次に、マスター鍵生成部１１０は、処理装置により、数１３２を計算する

。

[数132]

$$\begin{aligned}
&\text{for } t=1,\ldots,d^{\mathsf{CP}},\\
&\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}} := (q,\mathbb{V}_t^{\mathsf{CP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{CP}},e) := \mathcal{G}_{\mathsf{dpvs}}(1^\lambda,N_t^{\mathsf{CP}},\mathsf{param}_{\mathbb{G}}),\\
&X_t^{\mathsf{CP}} := (\chi_{t,i,j}^{\mathsf{CP}})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t^{\mathsf{CP}},\mathbb{F}_q),\\
&(\nu_{t,i,j}^{\mathsf{CP}})_{i,j} := \psi\cdot((X_t^{\mathsf{CP}})^{\mathrm{T}})^{-1},\\
&b_{t,i}^{\mathsf{CP}} := (\chi_{t,i,1}^{\mathsf{CP}},\ldots,\chi_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{\mathsf{CP}} := (b_{t,1}^{\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{\mathsf{CP}}),\\
&b_{t,i}^{*\mathsf{CP}} := (\nu_{t,i,1}^{\mathsf{CP}},\ldots,\nu_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{*\mathsf{CP}} := (b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{*\mathsf{CP}})
\end{aligned}$$

つまり、マスター鍵生成部１１０は、ｔ＝１，．．．，ｄ^{CP}の各整数ｔについて以下の処理を実行する。

マスター鍵生成部１１０は、入力したセキュリティパラメータλ（１$^{\lambda}$）と、設定したＮ$_{t}^{CP}$と、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$_{VtCP}$：＝（ｑ，Ｖ$_{t}^{CP}$，Ｇ$_{T}$，Ａ$_{t}^{CP}$，ｅ）の値を生成する。

また、マスター鍵生成部１１０は、設定したＮ$_{t}^{CP}$と、Ｆ$_{q}$とを入力として、線形変換Ｘ$_{t}^{CP}$：＝（$\chi_{t}^{CP}$$_{,i,j}$）$_{i,j}$をランダムに生成する。（$\chi_{t}^{CP}$$_{,i,j}$）$_{i,j}$は、行列$\chi_{t}^{CP}$$_{,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}^{CP}$である。

また、マスター鍵生成部１１０は、乱数ϕと線形変換Ｘ$_{t}^{CP}$とに基づき、（$\nu_{t}^{CP}$$_{,i,j}$）$_{i,j}$：＝$\phi$・（（Ｘ$_{t}^{CP}$）^{T}）$^{-1}$を生成する。なお、（$\nu_{t}^{CP}$$_{,i,j}$）$_{i,j}$も（$\chi_{t}^{CP}$$_{,i,j}$）$_{i,j}$と同様に、行列$\nu_{t}^{CP}$$_{,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}^{CP}$である。

そして、マスター鍵生成部１１０は、線形変換Ｘ$_{t}^{CP}$に基づき、標準基底Ａ$_{t}^{CP}$から基底Ｂ$_{t}^{CP}$を生成する。同様に、マスター鍵生成部１１０は、（$\nu_{t}^{CP}$$_{,i,j}$）$_{i,j}$に基づき、標準基底Ａ$_{t}^{CP}$から基底Ｂ＊$_{t}^{CP}$を生成する。

[0049] 次に、マスター鍵生成部１１０は、処理装置により、数１３３を計算する。

[数133]

$$g_T := e(g,g)^{\psi},$$
$$\mathrm{param}_{\vec{n}} := (\mathrm{param}_{\mathbb{V}_0}, \{\mathrm{param}_{\mathbb{V}_t^{KP}}\}_{t=1,\ldots,d^{KP}}, \{\mathrm{param}_{\mathbb{V}_t^{CP}}\}_{t=1,\ldots,d^{CP}}, g_T)$$

つまり、マスター鍵生成部１１０は、g_Tにｅ（ｇ，ｇ）$^{\psi}$を設定する。

また、マスター鍵生成部１１０は、$\mathrm{param}_{\vec{n}}$にparam_{V0}と、ｔ＝１，．．．，d^{KP}の各整数ｔについてのparam_{VtKP}と、ｔ＝１，．．．，d^{CP}の各整数ｔについてのparam_{VtCP}と、g_Tとを設定する。なお、ｉ＝１，．．．，N_0の各整数ｉについて、g_T＝ｅ（$b_{0,i}$，$b^*_{0,i}$）である。また、ｔ＝１，．．．，d^{KP}とｉ＝１，．．．，N_t^{KP}との各整数ｔ，ｉについて、g_T＝ｅ（$b_{t,i}$，$b^*_{t,i}$）である。また、ｔ＝１，．．．，d^{CP}とｉ＝１，．．．，N_t^{CP}との各整数ｔ，ｉについて、g_T＝ｅ（$b_{t,i}$，$b^*_{t,i}$）である。

[0050] そして、マスター鍵生成部１１０は、$\mathrm{param}_{\vec{n}}$と、{B_0、B^*_0}と、ｔ＝１，．．．，d^{KP}の各整数ｔについての{B_t^{KP}、$B^*_t{}^{KP}$}と、ｔ＝１，．．．，d^{CP}の各整数ｔについての{B_t^{CP}、$B^*_t{}^{CP}$}とを得る。

[0051] （Ｓ１０２：公開パラメータ生成ステップ）

マスター鍵生成部１１０は、処理装置により、基底B_0の部分基底$\hat{B}_0$と、ｔ＝１，．．．，d^{KP}の各整数ｔについて、基底B_t^{KP}の部分基底$\hat{B}_t^{KP}$と、ｔ＝１，．．．，d^{CP}の各整数ｔについて、基底B_t^{CP}の部分基底$\hat{B}_t^{CP}$とを数１３４に示すように生成する。

[数134]

$$\hat{\mathbb{B}}_0 := (b^*_{0,1}, b^*_{0,2}, b^*_{0,2+u_0+1}, b^*_{0,2+u_0+1+w_0+1}, \ldots, b^*_{0,2+u_0+1+w_0+z_0}),$$
$$\text{for } t = 1, \ldots, d^{\mathsf{KP}},$$
$$\hat{\mathbb{B}}^{\mathsf{KP}}_t := (b^{\mathsf{KP}}_{t,1}, \ldots, b^{\mathsf{KP}}_{t,n^{\mathsf{KP}}_t}, b^{\mathsf{KP}}_{t,n^{\mathsf{KP}}_t+u^{\mathsf{KP}}_t+w^{\mathsf{KP}}_t+1}, \ldots, b^{\mathsf{KP}}_{t,n^{\mathsf{KP}}_t+u^{\mathsf{KP}}_t+w^{\mathsf{KP}}_t+z^{\mathsf{KP}}_t}),$$
$$\text{for } t = 1, \ldots, d^{\mathsf{CP}},$$
$$\hat{\mathbb{B}}^{\mathsf{CP}}_t := (b^{\mathsf{CP}}_{t,1}, \ldots, b^{\mathsf{CP}}_{t,n^{\mathsf{CP}}_t}, b^{\mathsf{CP}}_{t,n^{\mathsf{CP}}_t+u^{\mathsf{CP}}_t+w^{\mathsf{CP}}_t+1}, \ldots, b^{\mathsf{CP}}_{t,n^{\mathsf{CP}}_t+u^{\mathsf{CP}}_t+w^{\mathsf{CP}}_t+z^{\mathsf{CP}}_t})$$

マスター鍵生成部１１０は、生成した部分基底Ｂ＾$_0$，部分基底Ｂ＾$_t{}^{KP}$，部分基底Ｂ＾$_t{}^{CP}$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$_{n\to}$とを合わせて、公開パラメータｐｋとする。

[0052] （Ｓ１０３：マスター鍵生成ステップ）

マスター鍵生成部１１０は、処理装置により、基底Ｂ＊$_0$の部分基底Ｂ＾＊$_0$と、ｔ＝１，．．．，ｄ^{KP}の各整数ｔについて、基底Ｂ＊$_t{}^{KP}$の部分基底Ｂ＾＊$_t{}^{KP}$と、ｔ＝１，．．．，ｄ^{CP}の各整数ｔについて、基底Ｂ＊$_t{}^{CP}$の部分基底Ｂ＾＊$_t{}^{CP}$とを数１３５に示すように生成する。

[数135]

$$\hat{\mathbb{B}}^*_0 := (b^*_{0,1}, b^*_{0,2}, b^*_{0,2+u_0+1}, b^*_{0,2+u_0+1+1}, \ldots, b^*_{0,2+u_0+1+w_0}),$$
$$\text{for } t = 1, \ldots, d^{\mathsf{KP}},$$
$$\hat{\mathbb{B}}^{*\mathsf{KP}}_t := (b^{*\mathsf{KP}}_{t,1}, \ldots, b^{*\mathsf{KP}}_{t,n^{\mathsf{KP}}_t}, b^{*\mathsf{KP}}_{t,n^{\mathsf{KP}}_t+u^{\mathsf{KP}}_t+1}, \ldots, b^{*\mathsf{KP}}_{t,n^{\mathsf{KP}}_t+u^{\mathsf{KP}}_t+w^{\mathsf{KP}}_t}),$$
$$\text{for } t = 1, \ldots, d^{\mathsf{CP}},$$
$$\hat{\mathbb{B}}^{*\mathsf{CP}}_t := (b^{*\mathsf{CP}}_{t,1}, \ldots, b^{*\mathsf{CP}}_{t,n^{\mathsf{CP}}_t}, b^{*\mathsf{CP}}_{t,n^{\mathsf{CP}}_t+u^{\mathsf{CP}}_t+1}, \ldots, b^{*\mathsf{CP}}_{t,n^{\mathsf{CP}}_t+u^{\mathsf{CP}}_t+w^{\mathsf{CP}}_t})$$

マスター鍵生成部１１０は、生成した部分基底Ｂ＾＊$_0$，部分基底Ｂ＾＊$_t{}^{KP}$，部分基底Ｂ＾＊$_t{}^{CP}$をマスター鍵ｓｋとする。

[0053] （Ｓ１０４：マスター鍵記憶ステップ）

マスター鍵記憶部１２０は、（Ｓ１０２）で生成した公開パラメータｐｋ

を記憶装置に記憶する。また、マスター鍵記憶部１２０は、（Ｓ１０３）で生成したマスター鍵ｓｋを記憶装置に記憶する。

[0054] つまり、（Ｓ１０１）から（Ｓ１０３）において、鍵生成装置１００は数１３６に示すＳｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター鍵ｓｋとを生成する。そして、（Ｓ１０４）で、鍵生成装置１００は生成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、公開パラメータは、例えば、ネットワークを介して公開され、暗号化装置２００や復号装置３００が取得可能な状態にされる。

[数136]

$$
\begin{aligned}
&\mathsf{Setup}(1^{\lambda},\vec{n} := ((d^{\mathsf{KP}};n_t^{\mathsf{KP}},u_t^{\mathsf{KP}},w_t^{\mathsf{KP}},z_t^{\mathsf{KP}}\left(t=1,...,d^{\mathsf{KP}}\right)),\\
&\qquad\qquad (d^{\mathsf{CP}};n_t^{\mathsf{CP}},u_t^{\mathsf{CP}},w_t^{\mathsf{CP}},z_t^{\mathsf{CP}}\left(t=1,...,d^{\mathsf{CP}}\right))):\\
&\quad(\mathsf{param}_{\vec{n}},\mathbb{B}_0,\mathbb{B}_0^*,\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\\
&\quad\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})\xleftarrow{\mathsf{R}}\mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}),\\
&\quad\hat{\mathbb{B}}_0 := (b_{0,1}^*,b_{0,2}^*,b_{0,2+u_0+1}^*,b_{0,2+u_0+1+w_0+1}^*,\ldots,b_{0,2+u_0+1+w_0+z_0}^*),\\
&\quad\hat{\mathbb{B}}_0^* := (b_{0,1}^*,b_{0,2}^*,b_{0,2+u_0+1}^*,b_{0,2+u_0+1+1}^*,\ldots,b_{0,2+u_0+1+w_0}^*),\\
&\quad\text{for } t=1,\ldots,d^{\mathsf{KP}},\\
&\quad\hat{\mathbb{B}}_t^{\mathsf{KP}} := (b_{t,1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}},b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}}}^{\mathsf{KP}}),\\
&\quad\hat{\mathbb{B}}_t^{*\mathsf{KP}} := (b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{*\mathsf{KP}},b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}}^{*\mathsf{KP}}),\\
&\quad\text{for } t=1,\ldots,d^{\mathsf{CP}},\\
&\quad\hat{\mathbb{B}}_t^{\mathsf{CP}} := (b_{t,1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}},b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}}}^{\mathsf{CP}}),\\
&\quad\hat{\mathbb{B}}_t^{*\mathsf{CP}} := (b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{*\mathsf{CP}},b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}}^{*\mathsf{CP}}),\\
&\quad\mathsf{pk} := (1^{\lambda},\mathsf{param}_{\vec{n}},\hat{\mathbb{B}}_0,\{\hat{\mathbb{B}}_t^{\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}),\\
&\quad\mathsf{sk} := (\hat{\mathbb{B}}_0^*,\{\hat{\mathbb{B}}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})\\
&\quad\mathsf{return\ pk, sk.}
\end{aligned}
$$

[0055] 次に、図１０に基づき、ＫｅｙＧｅｎアルゴリズムの処理について説明する。

（Ｓ２０１：情報入力ステップ）

第１ＫＰ情報入力部１３１は、入力装置により、アクセスストラクチャS^{KP}：＝（M^{KP}，ρ^{KP}）を入力する。なお、行列M^{KP}は、L^{KP}行×r^{KP}列の行列である。L^{KP}，r^{KP}は、１以上の整数である。

また、第１ＣＰ情報入力部１３２は、入力装置により、属性の集合Γ^{CP}：＝｛（ｔ，$\vec{x}_t^{CP}$：＝（$x_{t,i}^{CP}$（ｉ＝１，．．．，n_t^{CP}））∈$F_q^{nt^{CP}}$＼｛$\vec{0}$｝）｜１≦ｔ≦d^{CP}｝を入力する。ｔは、１以上d^{CP}以下の全ての整数ではなく、１以上d^{CP}以下の少なくとも一部の整数であってもよい。

なお、アクセスストラクチャS^{KP}の行列M^{KP}の設定については、実現したいシステムの条件に応じて設定されるものである。また、アクセスストラクチャS^{KP}のρ^{KP}や属性の集合Γ^{CP}は、例えば、復号鍵$sk_{(SKP,\Gamma CP)}$の使用者の属性情報が設定されている。

[0056] （Ｓ２０２：ｆベクトル生成ステップ）

ｆベクトル生成部１４１は、処理装置により、r^{KP}個の要素を有するベクトル$\vec{f}^{KP}$を数１３７に示すようにランダムに生成する。

[数137]

$$\vec{f}^{KP} \xleftarrow{U} \mathbb{F}_q^{r^{KP}}$$

[0057] （Ｓ２０３：ｓベクトル生成ステップ）

ｓベクトル生成部１４２は、処理装置により、（Ｓ２０１）で入力したアクセスストラクチャS^{KP}に含まれる（L^{KP}行×r^{KP}列）の行列M^{KP}と、（Ｓ２０２）で生成したr^{KP}個の要素を有するベクトル$\vec{f}^{KP}$とに基づき、ベクトル$(\vec{s}^{KP})^T$を数１３８に示すように生成する。

[数138]

$$(\vec{s}^{KP})^T := (s_1^{KP},\ldots,s_{L^{KP}}^{KP})^T := M^{KP}\cdot(\vec{f}^{KP})^T$$

また、ｓベクトル生成部１４２は、処理装置により、（Ｓ２０２）で生成したベクトル$\vec{f}^{KP}$に基づき、値s_0^{KP}を数１３９に示すように生成する。な

お、１→は、全ての要素が値１のベクトルである。

[数139]

$$s_0^{KP} := \vec{1} \cdot (\vec{f}^{KP})^{T}$$

[0058] （Ｓ２０４：乱数生成ステップ）

乱数生成部１４３は、処理装置により、乱数δ^{CP}と、Γ^{CP}に含まれる（ｔ，$\vec{x}_t^{CP}$）の各整数ｔについて乱数$\vec{\eta}_t^{CP}$と、乱数$\vec{\eta}_0$とを数１４０に示すように生成する。

[数140]

$$\delta^{CP} \xleftarrow{U} \mathbb{F}_q,$$

$$\vec{\eta}_t^{CP} := (\eta_{t,1}^{CP},\ldots,\eta_{t,w_t^{CP}}^{CP}) \xleftarrow{U} \mathbb{F}_q^{w_t^{CP}} \quad \text{such that } (t,\vec{x}_t^{CP}) \in \Gamma^{CP},$$

$$\vec{\eta}_0 := (\eta_{0,1},\ldots,\eta_{0,w_0}) \xleftarrow{U} \mathbb{F}_q^{w_0}$$

[0059] （Ｓ２０５：主復号鍵生成ステップ）

主復号鍵生成部１４４は、処理装置により、復号鍵ｓｋ$_{(SKP,\ \Gamma CP)}$の要素である主復号鍵ｋ*$_0$を数１４１に示すように生成する。

[数141]

$$k_0^* := (-s_0^{KP}, \delta^{CP}, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*}$$

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１４１は、以下のように、基底Ｂ*$_0$の基底ベクトルの係数が設定されることを意味する。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$-s_0^{KP}$が設定される。基底ベクトル２の係数として乱数δ^{CP}が設定される。基底ベクトル$2+1,\ldots,2+u_0$の係数として０が設定される。基底ベクトル$2+u_0+1$の係数として１が設定される。基底ベクトル$2+u_0+1+1,\ldots,2+u_0+1+w_0$の係数として乱数$\eta_{0,1},\ldots,\eta_{0,w0}$（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$2+u_0+1+w_0+1,\ldots,2+u_0+1+w_0+z_0$の係数として０が設定される。

[0060] （Ｓ２０６：ＫＰ復号鍵生成ステップ）

ＫＰ復号鍵生成部１４５は、処理装置により、$i=1,\ldots,L^{KP}$の各整数ｉについて、復号鍵$sk_{(SKP,\Gamma CP)}$の要素であるＫＰ復号鍵$k^*_i{}^{KP}$を数１４２に示すように生成する。

[数142]

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

$$\text{if } \rho^{KP}(i)=(t,\vec{v}_i^{KP}:=(v_{i,1}^{KP},\ldots,v_{i,n_t^{KP}}^{KP})\in\mathbb{F}_q^{n_t^{KP}}\setminus\{\vec{0}\}),$$

$$\theta_i^{KP}\xleftarrow{U}\mathbb{F}_q,\ \vec{\eta}_i^{KP}:=(\eta_{i,1}^{KP},\ldots,\eta_{i,w_t^{KP}}^{KP})\xleftarrow{U}\mathbb{F}_q^{w_t^{KP}},$$

$$k_i^{*KP}:=(\overbrace{s_i^{KP}\vec{e}_{t,1}^{KP}+\theta_i^{KP}\vec{v}_i^{KP}}^{n_t^{KP}},\overbrace{0^{u_t^{KP}},}^{u_t^{KP}}\overbrace{\vec{\eta}_i^{KP},}^{w_t^{KP}}\overbrace{0^{z_t^{KP}}}^{z_t^{KP}})_{\mathbb{B}_t^{*KP}},$$

$$\text{if } \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP}),$$

$$\vec{\eta}_i^{KP}:=(\eta_{i,1}^{KP},\ldots,\eta_{i,w_t^{KP}}^{KP})\xleftarrow{U}\mathbb{F}_q^{w_t^{KP}},$$

$$k_i^{*KP}:=(\overbrace{s_i^{KP}\vec{v}_i^{KP}}^{n_t^{KP}},\overbrace{0^{u_t^{KP}},}^{u_t^{KP}}\overbrace{\vec{\eta}_i^{KP},}^{w_t^{KP}}\overbrace{0^{z_t^{KP}}}^{z_t^{KP}})_{\mathbb{B}_t^{*KP}}$$

つまり、数１４２は、数１４１と同様に、以下のように、基底$B^*_t{}^{KP}$の基底ベクトルの係数が設定されることを意味する。なお、ここでは、表記を簡略化して、基底ベクトル$b^*_{t,i}{}^{KP}$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$b^*_{t,1}{}^{KP}$を意味する。また、基底ベクトル$1,\ldots,3$であれば、基底ベクトル$b^*_{t,1}{}^{KP}$,

．．．，ｂ＊$_{t,3}^{KP}$を意味する。

ρ^{KP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{KP}$）である場合には、基底ベクトル１の係数として$s_i^{KP}+\theta_i^{KP}v_{i,1}^{KP}$が設定される。なお、上述したように、$\vec{e}_{t,j}^{KP}$は、数１１２に示す正規基底ベクトルを示す。また、基底ベクトル２，．．．，n_t^{KP}の係数として$\theta_i^{KP}v_{i,2}^{KP}$，．．．，$\theta_i^{KP}v_{i,ntKP}^{KP}$（ここで、ｎｔＫＰは$n_t^{KP}$のことである）が設定される。基底ベクトル$n_t^{KP}+1$，．．．，$n_t^{KP}+u_t^{KP}$の係数として０が設定される。基底ベクトル$n_t^{KP}+u_t^{KP}+1$，．．．，$n_t^{KP}+u_t^{KP}+w_t^{KP}$の係数として$\eta_{i,1}^{KP}$，．．．，$\eta_{i,wtKP}^{KP}$（ここで、ｗｔＫＰは$w_t^{KP}$のことである）が設定される。基底ベクトル$n_t^{KP}+u_t^{KP}+w_t^{KP}+1$，．．．，$n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$の係数として０が設定される。

一方、ρ^{KP}（ｉ）が否定形の組￢（ｔ，$\vec{v}_i^{KP}$）である場合には、基底ベクトル１，．．．，n_t^{KP}の係数として$s_i^{KP}v_{i,1}^{KP}$，．．．，$s_i^{KP}v_{i,ntKP}^{KP}$（ここで、ｎｔＫＰはn_t^{KP}のことである）が設定される。基底ベクトル$n_t^{KP}+1$，．．．，$n_t^{KP}+u_t^{KP}$の係数として０が設定される。基底ベクトル$n_t^{KP}+u_t^{KP}+1$，．．．，$n_t^{KP}+u_t^{KP}+w_t^{KP}$の係数として$\eta_{i,1}^{KP}$，．．．，$\eta_{i,wtKP}^{KP}$（ここで、ｗｔＫＰは$w_t^{KP}$のことである）が設定される。基底ベクトル$n_t^{KP}+u_t^{KP}+w_t^{KP}+1$，．．．，$n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$の係数として０が設定される。

なお、θ_i^{KP}及び$\vec{\eta}_i^{KP}$は乱数生成部１４３によって生成される乱数である。

[0061] （Ｓ２０７：ＣＰ復号鍵生成ステップ）

ＣＰ復号鍵生成部１４６は、処理装置により、Γ^{CP}に含まれる（ｔ，$\vec{x}_t^{CP}$）の各整数ｔについて、復号鍵$sk_{(SKP,\Gamma CP)}$の要素であるＣＰ復号鍵ｋ＊$_t^{CP}$を数１４３に示すように生成する。

[数143]

$$k_t^{*CP} := (\overbrace{\delta^{CP}\vec{x}_t^{CP}}^{n_t^{CP}}, \overbrace{0^{u_t^{CP}}}^{u_t^{CP}}, \overbrace{\vec{\eta}_t^{CP}}^{w_t^{CP}}, \overbrace{0^{z_t^{KP}}}^{z_t^{CP}})_{\mathbb{B}_t^{*CP}} \quad \text{for } (t, \vec{x}_t^{CP}) \in \Gamma^{CP}$$

つまり、数１４３は、数１４１と同様に、以下のように、基底Ｂ＊$_t^{CP}$の基底ベクトルの係数が設定されることを意味する。なお、ここでは、表記を簡略化して、基底ベクトルｂ＊$_{t,i}^{CP}$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＊$_{t,1}^{CP}$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＊$_{t,1}^{CP}$，．．．，ｂ＊$_{t,3}^{CP}$を意味する。

基底ベクトル１，．．．，ｎ$_t^{CP}$の係数として$\delta^{CP}x_{t,1}^{CP}$，．．．，$\delta^{CP}x_{t,ntCP}^{CP}$（ここで、ｎｔＣＰはｎ$_t^{CP}$のことである）が設定される。基底ベクトルｎ$_t^{CP}$＋１，．．．，ｎ$_t^{CP}$＋ｕ$_t^{CP}$の係数として０が設定される。基底ベクトルｎ$_t^{CP}$＋ｕ$_t^{CP}$＋１，．．．，ｎ$_t^{CP}$＋ｕ$_t^{CP}$＋ｗ$_t^{CP}$の係数として$\eta_{t,1}^{CP}$，．．．，$\eta_{t,wtCP}^{CP}$（ここで、ｗｔＣＰはｗ$_t^{CP}$のことである）が設定される。基底ベクトルｎ$_t^{CP}$＋ｕ$_t^{CP}$＋ｗ$_t^{CP}$＋１，．．．，ｎ$_t^{CP}$＋ｕ$_t^{CP}$＋ｗ$_t^{CP}$＋ｚ$_t^{CP}$の係数として０が設定される。

[0062] （Ｓ２０８：鍵配布ステップ）

鍵配布部１５０は、主復号鍵ｋ＊$_0$と、アクセスストラクチャＳ^{KP}及びＫＰ復号鍵ｋ＊$_i^{KP}$（ｉ＝１，．．．，Ｌ^{KP}）と、属性の集合Γ^{CP}及びＣＰ復号鍵ｋ＊$_t^{CP}$（ｔは属性の集合Γ^{CP}に含まれる（ｔ，ｘ→$_t^{CP}$）におけるｔ）とを要素とする復号鍵ｓｋ$_{(SKP,\Gamma CP)}$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$_{(SKP,\Gamma CP)}$は、他の方法により復号装置３００へ配布されてもよい。

[0063] つまり、（Ｓ２０１）から（Ｓ２０７）において、鍵生成装置１００は数１４４に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵ｓｋ$_{(SKP,\Gamma CP)}$を生成する。そして、（Ｓ２０８）で、鍵生成装置１００は生成された復号鍵ｓｋ$_{(SKP,\Gamma CP)}$を復号装置３００へ配布する。

[数144]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\mathbb{S}^{\mathsf{KP}}:=(M^{\mathsf{KP}},\rho^{\mathsf{KP}}),$$

$$\Gamma^{\mathsf{CP}}:=\{(t,\vec{x}_t^{\mathsf{CP}}:=(x_{t,1}^{\mathsf{CP}},\ldots,x_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}})\in\mathbb{F}_q^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})$$

$$\left|1\le t\le d^{\mathsf{CP}},x_{t,1}^{\mathsf{CP}}:=1\right\})$$

$$\vec{f}^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{r^{\mathsf{KP}}},\quad(\vec{s}^{\mathsf{KP}})^{\mathrm{T}}:=(s_1^{\mathsf{KP}},\ldots,s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}}:=M^{\mathsf{KP}}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{KP}}:=\vec{1}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$\delta^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_t^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t^{\mathsf{CP}}}\ \text{such that}\ (t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

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

$$k_0^*:=(-s_0^{\mathsf{KP}},\delta^{\mathsf{CP}},\overbrace{0^{u_0}}^{u_0},1,\overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0},\overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

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

$$\text{if}\ \rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}}:=(v_{i,1}^{\mathsf{KP}},\ldots,v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}})\in\mathbb{F}_q^{n_t^{\mathsf{KP}}}\setminus\{\vec{0}\}),$$

$$\theta_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{e}_{t,1}^{\mathsf{KP}}+\theta_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

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

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{for}\ (t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$k_t^{*\mathsf{CP}}:=(\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}},\overbrace{\vec{\eta}_t^{\mathsf{CP}}}^{w_t^{\mathsf{CP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{*\mathsf{CP}}},$$

$$\mathsf{return}\ \mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})}:=$$

$$(k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\}_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}}).$$

[0064] 暗号化装置２００の機能と動作とについて説明する。

図７に示すように、暗号化装置２００は、公開パラメータ取得部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（データ出力部）を備える。

また、情報入力部２２０は、ＫＰ情報入力部２２１（第２ＫＰ情報入力部）、ＣＰ情報入力部２２２（第２ＣＰ情報入力部）、メッセージ入力部２２３を備える。また、暗号化データ生成部２３０は、ｆベクトル生成部２３１、ｓベクトル生成部２３２、乱数生成部２３３、主暗号化データ生成部２３４、ＫＰ暗号化データ生成部２３５、ＣＰ暗号化データ生成部２３６、メッセージ暗号化データ生成部２３７を備える。

[0065] 図１１に基づき、Ｅｎｃアルゴリズムの処理について説明する。

（Ｓ３０１：公開パラメータ取得ステップ）

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

[0066] （Ｓ３０２：情報入力ステップ）

ＫＰ情報入力部２２１は、入力装置により、属性の集合Γ^{KP}：＝｛（ｔ，$\vec{x}_t^{KP}$：＝（$x_{t,i}^{KP}$（ｉ＝１，．．．，n_t^{KP}））$\in F_q^{n_t^{KP}} \setminus \{\vec{0}\}$）｜１≦ｔ≦$d^{KP}$｝を入力する。ｔは、１以上$d^{KP}$以下の全ての整数ではなく、１以上$d^{KP}$以下の少なくとも一部の整数であってもよい。

また、ＣＰ情報入力部２２２は、入力装置により、アクセスストラクチャS^{CP}：＝（M^{CP}，ρ^{CP}）を入力する。なお、行列M^{CP}は、L^{CP}行×r^{CP}列の行列である。L^{CP}，r^{CP}は、１以上の整数である。

また、メッセージ入力部は、入力装置により、復号装置３００へ送信するメッセージｍを入力する。

なお、アクセスストラクチャS^{CP}の行列M^{CP}の設定については、実現したいシステムの条件に応じて設定されるものである。アクセスストラクチャS^{CP}のρ^{CP}や属性の集合Γ^{KP}は、例えば、復号可能なユーザの属性情報が設定されている。

[0067] （Ｓ３０３：乱数生成ステップ）

乱数生成部２３３は、処理装置により、乱数ω^{KP}と、乱数$\vec{\phi}_0$と、Γ^{KP}に

含まれる（ｔ，ｘ$^{\rightarrow}{}_{t}{}^{KP}$）の各整数ｔについてφ$^{\rightarrow}{}_{t}{}^{KP}$と、乱数ζとを数１４５に示すように生成する。

[数145]

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

$$\vec{\varphi}_0 := (\varphi_{0,1},\ldots,\varphi_{0,z_0}) \xleftarrow{U} \mathbb{F}_q^{z_0},$$

$$\vec{\varphi}_t^{KP} := (\varphi_{t,1}^{KP},\ldots,\varphi_{t,z_t^{KP}}^{KP}) \xleftarrow{U} \mathbb{F}_q^{z_t^{KP}} \quad \text{for } (t,\vec{x}_t^{KP}) \in \Gamma$$

[0068] （Ｓ３０４：ｆベクトル生成ステップ）

ｆベクトル生成部２３１は、処理装置により、ｒ^{CP}個の要素を有するベクトルｆ$^{\rightarrow CP}$を数１４６に示すようにランダムに生成する。

[数146]

$$\vec{f}^{CP} \xleftarrow{R} \mathbb{F}_q^{r^{CP}}$$

[0069] （Ｓ３０５：ｓベクトル生成ステップ）

ｓベクトル生成部２３２は、処理装置により、（Ｓ３０２）で入力したアクセスストラクチャＳ^{CP}に含まれる（Ｌ^{CP}行×ｒ^{CP}列）の行列Ｍ^{CP}と、（Ｓ３０４）で生成したｒ^{CP}個の要素を有するベクトルｆ$^{\rightarrow CP}$とに基づき、ベクトル（ｓ$^{\rightarrow CP}$）^{T}を数１４７に示すように生成する。

[数147]

$$(\vec{s}^{CP})^{T} := (s_1^{CP},\ldots,s_{L^{CP}}^{CP})^{T} := M^{CP}\cdot(\vec{f}^{CP})^{T}$$

また、ｓベクトル生成部１４２は、処理装置により、（Ｓ３０４）で生成したベクトルｆ$^{\rightarrow CP}$に基づき、値ｓ$_{0}{}^{CP}$を数１４８に示すように生成する。なお、１$^{\rightarrow}$は、全ての要素が値１のベクトルである。

[数148]

$$s_0^{CP} := \vec{1}\cdot(\vec{f}^{CP})^{T}$$

[0070] （Ｓ３０６：主暗号化データ生成ステップ）

主暗号化データ生成部２３４は、処理装置により、暗号化データｃｔ$_{(\Gamma KP, SCP)}$の要素である主暗号化データｃ$_0$を数１４９に示すように生成する。

[数149]

$$c_0 := (\omega^{KP}, -s_0^{CP}, \overbrace{0^{u_0},}^{u_0} \zeta, \overbrace{0^{w_0},}^{w_0} \overbrace{\varphi_{0,1},\ldots,\varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0}$$

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１４９は、以下のように、基底Ｂ$_0$の基底ベクトルの係数が設定されることを意味する。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の係数として乱数ω^{KP}が設定される。基底ベクトル２の係数として－ｓ$_0{}^{CP}$が設定される。基底ベクトル２＋１，．．．，２＋ｕ$_0$の係数として０が設定される。基底ベクトル２＋ｕ$_0$＋１の係数として乱数ζが設定される。基底ベクトル２＋ｕ$_0$＋１＋１，．．．，２＋ｕ$_0$＋１＋ｗ$_0$の係数として０が設定される。基底ベクトル２＋ｕ$_0$＋１＋ｗ$_0$＋１，．．．，２＋ｕ$_0$＋１＋ｗ$_0$＋ｚ$_0$の係数として乱数$\phi_{0,1}$，．．．，$\phi_{0,z0}$（ここで、ｚ０はｚ$_0$のことである）が設定される。

[0071] （Ｓ３０７：ＫＰ暗号化データ生成ステップ）

ＫＰ暗号化データ生成部２３５は、処理装置により、Γ^{KP}に含まれる（ｔ，$x^{\rightarrow}{}_t{}^{KP}$）の各整数ｔについて、暗号化データｃｔ$_{(\Gamma KP, SCP)}$の要素であるＫＰ暗号化データｃ$_t{}^{KP}$を数１５０に示すように生成する。

[数150]

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

つまり、数１５０は、数１４９と同様に、以下のように、基底Ｂ$_t^{KP}$の基底ベクトルの係数が設定されることを意味する。なお、ここでは、表記を簡略化して、基底ベクトルｂ$_{t,i}^{KP}$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$_{t,1}^{KP}$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$_{t,1}^{KP}$，．．．，ｂ$_{t,3}^{KP}$を意味する。

基底ベクトル１，．．．，ｎ$_t^{KP}$の係数としてω^{KP}ｘ$_{t,1}^{KP}$，．．．，ω^{KP}ｘ$_{t,ntKP}^{KP}$（ここで、ｎｔＫＰはｎ$_t^{KP}$のことである）が設定される。基底ベクトルｎ$_t^{KP}$＋１，．．．，ｎ$_t^{KP}$＋ｕ$_t^{KP}$＋ｗ$_t^{KP}$の係数として０が設定される。基底ベクトルｎ$_t^{KP}$＋ｕ$_t^{KP}$＋ｗ$_t^{KP}$＋１，．．．，ｎ$_t^{KP}$＋ｕ$_t^{KP}$＋ｗ$_t^{KP}$＋ｚ$_t^{KP}$の係数としてφ$_{t,1}^{KP}$，．．．，φ$_{t,ztKP}^{KP}$（ここで、ｚｔＣＰはｚ$_t^{CP}$のことである）が設定される。

[0072] （Ｓ３０８：ＣＰ暗号化データ生成ステップ）

ＣＰ暗号化データ生成部２３６は、処理装置により、ｉ＝１，．．．，Ｌ^{CP}の各整数ｉについて、暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$の要素であるＣＰ暗号化データｃ$_i^{CP}$を数１５１に示すように生成する。

[数151]

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

$$\text{if } \rho^{\mathsf{CP}}(i)=(t,\vec{v}_i^{\mathsf{CP}}:=(v_{i,1}^{\mathsf{CP}},\ldots,v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}})\in\mathbb{F}_q^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})(v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}:=1),$$

$$\theta_i^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q\ ,\vec{\varphi}_i^{\mathsf{CP}}:=(\varphi_{i,0}^{\mathsf{CP}},\ldots,\varphi_{i,z_t^{\mathsf{CP}}}^{\mathsf{CP}})\xleftarrow{\mathsf{U}}\mathbb{F}_q^{z_t^{\mathsf{CP}}},$$

$$c_i^{\mathsf{CP}}:=(\overbrace{s_i^{\mathsf{CP}}\vec{e}_{t,1}^{\mathsf{CP}}+\theta_i^{\mathsf{CP}}\vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{u_t^{\mathsf{CP}}},}^{u_t^{\mathsf{CP}}}\overbrace{0^{w_t^{\mathsf{CP}}},}^{w_t^{\mathsf{CP}}}\overbrace{\vec{\varphi}_i^{\mathsf{CP}})}^{z_t^{\mathsf{CP}}}{}_{\mathbb{B}_t^{\mathsf{CP}}},$$

$$\text{if } \rho^{\mathsf{CP}}(i)=\neg(t,\vec{v}_i^{\mathsf{CP}}),$$

$$\vec{\varphi}_i^{\mathsf{CP}}:=(\varphi_{i,0}^{\mathsf{CP}},\ldots,\varphi_{i,z_t^{\mathsf{CP}}}^{\mathsf{CP}})\xleftarrow{\mathsf{U}}\mathbb{F}_q^{z_t^{\mathsf{CP}}},$$

$$c_i^{\mathsf{CP}}:=(\overbrace{s_i^{\mathsf{CP}}\vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{u_t^{\mathsf{CP}}},}^{u_t^{\mathsf{CP}}}\overbrace{0^{w_t^{\mathsf{CP}}},}^{w_t^{\mathsf{CP}}}\overbrace{\vec{\varphi}_i^{\mathsf{CP}})}^{z_t^{\mathsf{CP}}}{}_{\mathbb{B}_t^{\mathsf{CP}}}$$

つまり、数１５１は、数１５０と同様に、以下のように、基底Ｂ$_t{}^{CP}$の基底ベクトルの係数が設定されることを意味する。なお、ここでは、表記を簡略化して、基底ベクトルｂ$_{t,\ i}{}^{CP}$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$_{t,\ 1}{}^{CP}$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$_{t,\ 1}{}^{CP}$，．．．，ｂ$_{t,\ 3}{}^{CP}$を意味する。

ρ^{CP}（ｉ）が肯定形の組（ｔ，ｖ$\rightarrow_i{}^{CP}$）である場合には、基底ベクトル１の係数としてｓ$_i{}^{CP}$＋θ$_i{}^{CP}$ｖ$_{i,\ 1}{}^{CP}$が設定される。なお、上述したように、ｅ$\rightarrow_{t,\ j}{}^{CP}$は、数１１２に示す正規基底ベクトルを示す。また、基底ベクトル２，．．．，ｎ$_t{}^{CP}$の係数としてθ$_i{}^{CP}$ｖ$_{i,\ 2}{}^{CP}$，．．．，θ$_i{}^{CP}$ｖ$_{i,\ ntCP}{}^{CP}$（ここで、ｎｔＣＰはｎ$_t{}^{CP}$のことである）が設定される。基底ベクトルｎ$_t{}^{CP}$＋１，．．．，ｎ$_t{}^{CP}$＋ｕ$_t{}^{CP}$＋ｗ$_t{}^{CP}$の係数として０が設定される。基底ベクトルｎ$_t{}^{CP}$＋ｕ$_t{}^{CP}$＋ｗ$_t{}^{CP}$＋１，．．．，ｎ$_t{}^{CP}$＋ｕ$_t{}^{CP}$＋ｗ$_t{}^{CP}$＋ｚ$_t{}^{CP}$の係数としてφ$_{i,\ 1}{}^{CP}$，．．．，φ$_{i,\ ztCP}{}^{CP}$（ここで、ｚｔＣＰはｚ$_t{}^{CP}$のことである）が設定される。

一方、ρ^{CP}（ｉ）が否定形の組¬（ｔ，ｖ$\rightarrow_i{}^{CP}$）である場合には、基底ベ

クトル1，．．．，n_t^{CP}の係数として$s_i^{CP}v_{i,1}^{CP}$，．．．，$s_i^{CP}v_{i,n_{tCP}}^{CP}$（ここで、ｎｔＣＰは$n_t^{CP}$のことである）が設定される。基底ベクトル$n_t^{CP}+1$，．．．，$n_t^{CP}+u_t^{CP}+w_t^{CP}$の係数として０が設定される。基底ベクトル$n_t^{CP}+u_t^{CP}+w_t^{CP}+1$，．．．，$n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$の係数として$\phi_{i,1}^{CP}$，．．．，$\phi_{i,z_{tCP}}^{CP}$（ここで、ｚｔＣＰは$z_t^{CP}$のことである）が設定される。

なお、θ_i^{CP}及び$\vec{\phi}_i^{CP}$は乱数生成部２３３によって生成される乱数である。

[0073] （Ｓ３０９：メッセージ暗号化データ生成ステップ）

メッセージ暗号化データ生成部２３７は、処理装置により、暗号化データ$ct_{(\Gamma KP,SCP)}$の要素であるメッセージ暗号化データc_{d+1}を数１５２に示すように生成する。

[数152]

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

なお、上述したように、数１５３である。

[数153]

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

[0074] （Ｓ３１０：データ送信ステップ）

データ送信部２４０は、主暗号化データc_0と、属性の集合Γ^{KP}及びＫＰ暗号化データc_t^{KP}と、アクセスストラクチャS^{CP}及びＣＰ暗号化データc_i^{CP}と、メッセージ暗号化データc_{d+1}とを要素とする暗号化データ$ct_{(\Gamma KP,SCP)}$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$ct_{(\Gamma KP,SCP)}$は、他の方法により復号装置３００へ送信されてもよい。

[0075] つまり、（Ｓ３０１）から（Ｓ３０９）において、暗号化装置２００は、数１５４に示すＥｎｃアルゴリズムを実行して、暗号化データ$ct_{(\Gamma KP,SCP}$

) を生成する。そして、（Ｓ３１０）で、暗号化装置２００は、生成された暗号化データｃｔ$_{(\Gamma^{KP},\mathbb{S}^{CP})}$を復号装置３００へ送信する。

[数154]

$$
\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, m, \Gamma^{\mathsf{KP}} :=\\
&\quad \{(t, \vec{x}_t^{\mathsf{KP}} := (x_{t,1}^{\mathsf{KP}}, \ldots, x_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}) \in \mathbb{F}_q^{n_t^{\mathsf{KP}}} \setminus \{\vec{0}\}) \,\middle|\, 1 \le t \le d^{\mathsf{KP}}, x_{t,1}^{\mathsf{KP}} := 1\},\\
&\quad \mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}}, \rho^{\mathsf{CP}})):\\
&\qquad \omega^{\mathsf{KP}}, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0},\ \vec{\varphi}_t^{\mathsf{KP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t^{\mathsf{KP}}} \ \text{for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma,\\
&\qquad \vec{f}^{\mathsf{CP}} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{r^{\mathsf{CP}}}, (\vec{s}^{\mathsf{CP}})^{\mathrm{T}} := (s_1^{\mathsf{CP}}, \ldots, s_{L^{\mathsf{CP}}}^{\mathsf{CP}})^{\mathrm{T}} := M^{\mathsf{CP}} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad s_0^{\mathsf{CP}} := \vec{1} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, \overbrace{0^{u_0},}^{u_0} \zeta, \overbrace{0^{w_0},}^{w_0} \overbrace{\varphi_{0,1}, \ldots, \varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0},\\
&\qquad \text{for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}},\\
&\qquad c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}} \vec{x}_t^{\mathsf{KP}},}^{n_t^{\mathsf{KP}}} \overbrace{0^{u_t^{\mathsf{KP}}},}^{u_t^{\mathsf{KP}}} \overbrace{0^{w_t^{\mathsf{KP}}},}^{w_t^{\mathsf{KP}}} \overbrace{\vec{\varphi}_t^{\mathsf{KP}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{\mathsf{KP}}},\\
&\qquad \text{for } i = 1, \ldots, L^{\mathsf{CP}},\\
&\qquad \text{if } \rho^{\mathsf{CP}}(i) = (t, \vec{v}_i^{\mathsf{CP}} := (v_{i,1}^{\mathsf{CP}}, \ldots, v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}) \in \mathbb{F}_q^{n_t^{\mathsf{CP}}} \setminus \{\vec{0}\}),\\
&\qquad\quad \theta_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t^{\mathsf{CP}}},\\
&\qquad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{e}_{t,1}^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}},}^{n_t^{\mathsf{CP}}} \overbrace{0^{u_t^{\mathsf{CP}}},}^{u_t^{\mathsf{CP}}} \overbrace{0^{w_t^{\mathsf{CP}}},}^{w_t^{\mathsf{CP}}} \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad \text{if } \rho^{\mathsf{CP}}(i) = \neg(t, \vec{v}_i^{\mathsf{CP}}),\ \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t^{\mathsf{CP}}},\\
&\qquad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}},}^{n_t^{\mathsf{CP}}} \overbrace{0^{u_t^{\mathsf{CP}}},}^{u_t^{\mathsf{CP}}} \overbrace{0^{w_t^{\mathsf{CP}}},}^{w_t^{\mathsf{CP}}} \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad c_{d+1} := g_T^{\zeta} m,\\
&\qquad \text{return } \mathsf{ct}_{(\Gamma^{\mathsf{KP}}, \mathbb{S}^{\mathsf{CP}})} :=\\
&\qquad\quad (c_0; \Gamma^{\mathsf{KP}}, \{c_t^{\mathsf{KP}}\}_{(t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}}}; \mathbb{S}^{\mathsf{CP}}, c_1^{\mathsf{CP}}, \ldots, c_{L^{\mathsf{CP}}}^{\mathsf{CP}}; c_{d+1}).
\end{aligned}
$$

[0076] 復号装置３００の機能と動作とについて説明する。

図８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（データ取得部）、スパンプログラム計算部３３０、補完係数計算部３４０、ペアリング演算部３５０、メッセージ計算部３６０を備える。

また、スパンプログラム計算部３３０は、ＫＰスパンプログラム計算部３３１、ＣＰスパンプログラム計算部３３２を備える。また、補完係数計算部３４０は、ＫＰ補完係数計算部３４１、ＣＰ補完係数計算部３４２を備える。

[0077] 図１２に基づき、Ｄｅｃアルゴリズムの処理について説明する。

（Ｓ４０１：復号鍵取得ステップ）

復号鍵取得部３１０は、例えば、通信装置によりネットワークを介して、鍵生成装置１００から配布された復号鍵 $sk_{(S_{KP}, \Gamma_{CP})}$ 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。

[0078] （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 $ct_{(\Gamma_{KP}, S_{CP})}$ を受信する。

[0079] （Ｓ４０３：スパンプログラム計算ステップ）

ＫＰスパンプログラム計算部３３１は、処理装置により、（Ｓ４０１）で取得した復号鍵 $sk_{(S_{KP}, \Gamma_{CP})}$ に含まれるアクセスストラクチャ S^{KP} が、（Ｓ４０２）で受信した暗号化データ $ct_{(\Gamma_{KP}, S_{CP})}$ に含まれる属性の集合 Γ^{KP} を受理するか否かを判定する。

また、ＣＰスパンプログラム計算部３３２は、処理装置により、（Ｓ４０２）で受信した暗号化データ $ct_{(\Gamma_{KP}, S_{CP})}$ に含まれるアクセスストラクチャ S^{CP} が、（Ｓ４０１）で取得した復号鍵 $sk_{(S_{KP}, \Gamma_{CP})}$ に含まれる属性の集合 Γ^{CP} を受理するか否かを判定する。

なお、アクセスストラクチャが属性の集合を受理するか否かの判定方法は、「第３．関数型暗号を実現するための概念」で説明した通りである。

スパンプログラム計算部３３０は、アクセスストラクチャS^{KP}が属性の集合Γ^{KP}を受理し、かつ、アクセスストラクチャS^{CP}が属性の集合Γ^{CP}を受理する場合（Ｓ４０３で受理）、処理を（Ｓ４０４）へ進める。一方、アクセスストラクチャS^{KP}が属性の集合Γ^{KP}を拒絶する場合と、アクセスストラクチャS^{CP}が属性の集合Γ^{CP}を拒絶する場合との少なくともいずれかの場合（Ｓ４０３で拒絶）、暗号化データ$ct_{(\Gamma KP,\ SCP)}$を復号鍵$sk_{(SKP,\ \Gamma CP)}$で復号できないとして、識別情報⊥を出力して、処理を終了する。

[0080] （Ｓ４０４：補完係数計算ステップ）

ＫＰ補完係数計算部３４１は、処理装置により、数１５５となるI^{KP}と、I^{KP}に含まれる各整数ｉについて定数（補完係数）$\alpha_i{}^{KP}$とを計算する。

[数155]

$$\vec{1}=\sum_{i\in I}\alpha_i^{KP}M_i^{KP},\ \text{where } M_i^{KP} \text{ is the } i-\text{th row of } M^{KP}, \text{and}$$
$$I^{KP}\subseteq\{i\in\{1,\ldots,L^{KP}\}$$
$$\left|[\rho^{KP}(i)=(t,\vec{v}_i^{KP})\wedge(t,\vec{x}_t^{KP})\in\Gamma^{KP}\wedge\vec{v}_i^{KP}\cdot\vec{x}_t^{KP}=0]\right.$$
$$[\rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})\wedge(t,\vec{x}_t^{KP})\in\Gamma^{KP}\wedge\vec{v}_i^{KP}\cdot\vec{x}_t^{KP}\neq 0]\}$$

また、ＣＰ補完係数計算部３４２は、処理装置により、数１５６となるI^{CP}と、I^{CP}に含まれる各整数ｉについて定数（補完係数）$\alpha_i{}^{CP}$とを計算する。

[数156]

$$\vec{1}=\sum_{i\in I}\alpha_i^{CP}M_i^{CP},\ \text{where } M_i^{CP} \text{ is the } i-\text{th row of } M^{CP}, \text{and}$$
$$I^{CP}\subseteq\{i\in\{1,\ldots,L^{CP}\}$$
$$\left|[\rho^{CP}(i)=(t,\vec{v}_i^{CP})\wedge(t,\vec{x}_t^{CP})\in\Gamma^{CP}\wedge\vec{v}_i^{CP}\cdot\vec{x}_t^{CP}=0]\right.$$
$$[\rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})\wedge(t,\vec{x}_t^{CP})\in\Gamma^{CP}\wedge\vec{v}_i^{CP}\cdot\vec{x}_t^{CP}\neq 0]\}$$

[0081] （Ｓ４０５：ペアリング演算ステップ）

ペアリング演算部３５０は、処理装置により、数１５７を計算して、セッション鍵Ｋ＝$g_T{}^{\zeta}$を生成する。

[数157]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

なお、数１５８に示すように、数１５７を計算することにより鍵Ｋ＝g_T^{ζ}が得られる。

[数158]

$$
\begin{aligned}
K :=\ & e(c_0, k_0^*)\cdot \\
& \prod_{i\in I^{\mathsf{KP}}\wedge \rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}})} e(c_t^{\mathsf{KP}}, k_i^{*\mathsf{KP}})^{\alpha_i^{\mathsf{KP}}}\cdot \\
& \prod_{i\in I^{\mathsf{KP}}\wedge \rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}})} e(c_t^{\mathsf{KP}}, k_i^{*\mathsf{KP}})^{\alpha_i^{\mathsf{KP}}/(\vec{v}_i^{\mathsf{KP}}\cdot\vec{x}_t^{\mathsf{KP}})}\cdot \\
& \prod_{i\in I^{\mathsf{CP}}\wedge \rho^{\mathsf{CP}}(i)=(t,\vec{v}_i^{\mathsf{CP}})} e(c_t^{\mathsf{CP}}, k_i^{*\mathsf{CP}})^{\alpha_i^{\mathsf{CP}}}\cdot \\
& \prod_{i\in I^{\mathsf{CP}}\wedge \rho^{\mathsf{CP}}(i)=\neg(t,\vec{v}_i^{\mathsf{CP}})} e(c_t^{\mathsf{CP}}, k_i^{*\mathsf{CP}})^{\alpha_i^{\mathsf{CP}}/(\vec{v}_i^{\mathsf{CP}}\cdot\vec{x}_t^{\mathsf{CP}})} \\
=\ & g_T^{-\varpi^{\mathsf{KP}}s_0^{\mathsf{KP}}-\delta^{\mathsf{CP}}s_0^{\mathsf{CP}}+\zeta}\cdot \\
& \prod_{i\in I^{\mathsf{KP}}\wedge \rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}})} g_T^{\varpi^{\mathsf{KP}}\alpha_i s_i^{\mathsf{KP}}}\cdot \\
& \prod_{i\in I^{\mathsf{KP}}\wedge \rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}})} g_T^{\varpi^{\mathsf{KP}}\alpha_i s_i^{\mathsf{KP}}(\vec{v}_i^{\mathsf{KP}}\cdot\vec{x}_t^{\mathsf{KP}})/(\vec{v}_i^{\mathsf{KP}}\cdot\vec{x}_t^{\mathsf{KP}})}\cdot \\
& \prod_{i\in I^{\mathsf{CP}}\wedge \rho^{\mathsf{CP}}(i)=(t,\vec{v}_i^{\mathsf{CP}})} g_T^{\delta^{\mathsf{CP}}\alpha_i s_i^{\mathsf{CP}}}\cdot \\
& \prod_{i\in I^{\mathsf{CP}}\wedge \rho^{\mathsf{CP}}(i)=\neg(t,\vec{v}_i^{\mathsf{CP}})} g_T^{\delta^{\mathsf{CP}}\alpha_i s_i^{\mathsf{CP}}(\vec{v}_i^{\mathsf{CP}}\cdot\vec{x}_t^{\mathsf{CP}})/(\vec{v}_i^{\mathsf{CP}}\cdot\vec{x}_t^{\mathsf{CP}})} \\
=\ & g_T^{-\varpi^{\mathsf{KP}}s_0^{\mathsf{KP}}-\delta^{\mathsf{CP}}s_0^{\mathsf{CP}}+\zeta+\varpi^{\mathsf{KP}}s_0^{\mathsf{KP}}+\delta^{\mathsf{CP}}s_0^{\mathsf{CP}}} \\
=\ & g_T^{\zeta}
\end{aligned}
$$

[0082] （Ｓ４０６：メッセージ計算ステップ）

メッセージ計算部３６０は、処理装置により、m’＝c_{d+1}／Ｋを計算して、メッセージm’（＝m）を生成する。なお、メッセージ暗号化データc_{d+1}は数１５２に示す通りg_T^{ζ}mであり、Ｋはg_T^{ζ}であるから、m’＝c_{d+1}／Ｋを計算すればメッセージmが得られる。

[0083] つまり、（Ｓ４０１）から（Ｓ４０６）において、復号装置３００は、数１５９に示すＤｅｃアルゴリズムを実行して、メッセージm’（＝m）を生

成する。

[数159]

$$
\begin{aligned}
&\mathrm{Dec}(\mathrm{pk},\\
&\quad \mathrm{sk}_{(\mathbb{S}^{\mathrm{KP}},\Gamma^{\mathrm{CP}})} := (k_0^*;\mathbb{S}^{\mathrm{KP}},k_1^{*\mathrm{KP}},\ldots,k_{L^{\mathrm{KP}}}^{*\mathrm{KP}};\Gamma^{\mathrm{CP}},\{k_t^{*\mathrm{CP}}\})_{(t,\vec{x}_t^{\mathrm{CP}})\in\Gamma^{\mathrm{CP}}}),\\
&\quad \mathrm{ct}_{(\Gamma^{\mathrm{KP}},\mathbb{S}^{\mathrm{CP}})} := (c_0;\Gamma^{\mathrm{KP}},\{c_t^{\mathrm{KP}}\}_{(t,\vec{x}_t^{\mathrm{KP}})\in\Gamma^{\mathrm{KP}}};\mathbb{S}^{\mathrm{CP}},c_1^{\mathrm{CP}},\ldots,c_{L^{\mathrm{CP}}}^{\mathrm{CP}};c_{d+1})):\\
&\quad \text{If } \mathbb{S}^{\mathrm{KP}} := (M^{\mathrm{KP}},\rho^{\mathrm{KP}}) \text{ accepts } \Gamma^{\mathrm{KP}} := \{(t,\vec{x}_t^{\mathrm{KP}})\}\\
&\qquad \text{and } \mathbb{S}^{\mathrm{CP}} := (M^{\mathrm{CP}},\rho^{\mathrm{CP}}) \text{ accepts } \Gamma^{\mathrm{CP}} := \{(t,\vec{x}_t^{\mathrm{CP}})\},\\
&\quad \text{then compute } (I^{\mathrm{KP}},\{\alpha_i^{\mathrm{KP}}\}_{i\in I^{\mathrm{KP}}}) \text{ and } (I^{\mathrm{CP}},\{\alpha_i^{\mathrm{CP}}\}_{i\in I^{\mathrm{CP}}}) \text{ such that}\\
&\qquad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{\mathrm{KP}} M_i^{\mathrm{KP}}, \text{ where } M_i^{\mathrm{KP}} \text{ is the } i-\text{th row of } M^{\mathrm{KP}}, \text{and}\\
&\qquad I^{\mathrm{KP}} \subseteq \{i\in\{1,\ldots,L^{\mathrm{KP}}\}\\
&\qquad\quad \left|[\rho^{\mathrm{KP}}(i)=(t,\vec{v}_i^{\mathrm{KP}})\wedge(t,\vec{x}_t^{\mathrm{KP}})\in\Gamma^{\mathrm{KP}}\wedge\vec{v}_i^{\mathrm{KP}}\cdot\vec{x}_t^{\mathrm{KP}}=0]\right.\\
&\qquad\quad \vee[\rho^{\mathrm{KP}}(i)=\neg(t,\vec{v}_i^{\mathrm{KP}})\wedge(t,\vec{x}_t^{\mathrm{KP}})\in\Gamma^{\mathrm{KP}}\wedge\vec{v}_i^{\mathrm{KP}}\cdot\vec{x}_t^{\mathrm{KP}}\neq 0]\}, \text{and}\\
&\qquad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{\mathrm{CP}} M_i^{\mathrm{CP}}, \text{ where } M_i^{\mathrm{CP}} \text{ is the } i-\text{th row of } M^{\mathrm{CP}}, \text{and}\\
&\qquad I^{\mathrm{CP}} \subseteq \{i\in\{1,\ldots,L^{\mathrm{CP}}\}\\
&\qquad\quad \left|[\rho^{\mathrm{CP}}(i)=(t,\vec{v}_i^{\mathrm{CP}})\wedge(t,\vec{x}_t^{\mathrm{CP}})\in\Gamma^{\mathrm{CP}}\wedge\vec{v}_i^{\mathrm{CP}}\cdot\vec{x}_t^{\mathrm{CP}}=0]\right.\\
&\qquad\quad \vee[\rho^{\mathrm{CP}}(i)=\neg(t,\vec{v}_i^{\mathrm{CP}})\wedge(t,\vec{x}_t^{\mathrm{CP}})\in\Gamma^{\mathrm{CP}}\wedge\vec{v}_i^{\mathrm{CP}}\cdot\vec{x}_t^{\mathrm{CP}}\neq 0]\},\\
&\quad K := e(c_0,k_0^*)\cdot\\
&\qquad \prod_{i\in I^{\mathrm{KP}}\wedge\rho^{\mathrm{KP}}(i)=(t,\vec{v}_i^{\mathrm{KP}})} e(c_t^{\mathrm{KP}},k_i^{*\mathrm{KP}})^{\alpha_i^{\mathrm{KP}}}\cdot\\
&\qquad \prod_{i\in I^{\mathrm{KP}}\wedge\rho^{\mathrm{KP}}(i)=\neg(t,\vec{v}_i^{\mathrm{KP}})} e(c_t^{\mathrm{KP}},k_i^{*\mathrm{KP}})^{\alpha_i^{\mathrm{KP}}/(\vec{v}_i^{\mathrm{KP}}\cdot\vec{x}_t^{\mathrm{KP}})}\cdot\\
&\qquad \prod_{i\in I^{\mathrm{CP}}\wedge\rho^{\mathrm{CP}}(i)=(t,\vec{v}_i^{\mathrm{CP}})} e(c_t^{\mathrm{CP}},k_i^{*\mathrm{CP}})^{\alpha_i^{\mathrm{CP}}}\cdot\\
&\qquad \prod_{i\in I^{\mathrm{CP}}\wedge\rho^{\mathrm{CP}}(i)=\neg(t,\vec{v}_i^{\mathrm{CP}})} e(c_t^{\mathrm{CP}},k_i^{*\mathrm{CP}})^{\alpha_i^{\mathrm{CP}}/(\vec{v}_i^{\mathrm{CP}}\cdot\vec{x}_t^{\mathrm{CP}})},\\
&\quad \text{return } m' := c_{d+1}/K.
\end{aligned}
$$

[0084] 以上のように、暗号処理システム１０は、スパンプログラムと内積述語と秘密分散とを用いて構成したアクセスストラクチャ$\mathbb{S}^{\mathrm{KP}}$及び$\mathbb{S}^{\mathrm{CP}}$を用いて、暗号方式（関数型暗号方式）を実現する。したがって、暗号処理システム１

０は、非常に高い自由度でアクセス制御の設計を行うことが可能な暗号方式を実現する。

特に、暗号処理システム１０は、アクセスストラクチャS^{KP}を復号鍵に持たせ、アクセスストラクチャS^{CP}を暗号化データに持たせている。したがって、暗号処理システム１０は、復号鍵と暗号化データとの両方でアクセスコントロールを行うことができる。

[0085] なお、上記説明において、u_t、w_t、z_t（$t=0,\ldots,d+1$）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（$t=0,\ldots,d+1$）をそれぞれ０として、u_t、w_t、z_t（$t=0,\ldots,d+1$）の次元を設けなくてもよい。

[0086] また、上記説明では、（Ｓ１０１）でN_0に$2+u_0+1+w_0+z_0$を設定した。しかし、$2+u_0+1+w_0+z_0$を$2+2+1+2+1$として、N_0に８を設定してもよい。

また、上記説明では、（Ｓ１０１）でN_t^{KP}に$n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$を設定した。しかし、$n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$を$n_t^{KP}+n_t^{KP}+n_t^{KP}+1$として、$N_t^{KP}$に$3n_t^{KP}+1$を設定してもよい。

同様に、（Ｓ１０１）でN_t^{CP}に$n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$を設定した。しかし、$n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$を$n_t^{CP}+n_t^{CP}+n_t^{CP}+1$として、$N_t^{CP}$に$3n_t^{CP}+1$を設定してもよい。

この場合、数１３６に示すＳｅｔｕｐアルゴリズムは、数１６０のように書き換えられる。なお、$G_{o_b}^{UP}$は数１６１のように書き換えられる。

[数160]

$$\mathsf{Setup}(1^{\lambda}, \vec{n} := ((d^{\mathsf{KP}}; n_1^{\mathsf{KP}}, \ldots, n_{d^{\mathsf{KP}}}^{\mathsf{KP}}), (d^{\mathsf{CP}}; n_1^{\mathsf{CP}}, \ldots, n_{d^{\mathsf{CP}}}^{\mathsf{CP}}))):$$

$$(\mathsf{param}_{\vec{n}}, \mathbb{B}_0, \mathbb{B}_0^*, \{\mathbb{B}_t^{\mathsf{KP}}, \mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},$$

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

$$\hat{\mathbb{B}}_0 := (b_{0,1}, b_{0,2}, b_{0,5}, b_{0,8}), \quad \hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,2}^*, b_{0,5}^*, b_{0,6}^*, b_{0,7}^*),$$

$$\text{for } t = 1, \ldots, d^{\mathsf{KP}}, \quad \hat{\mathbb{B}}_t^{\mathsf{KP}} := (b_{t,1}^{\mathsf{KP}}, \ldots, b_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}, b_{t,3n_t^{\mathsf{KP}}+1}^{\mathsf{KP}}),$$

$$\hat{\mathbb{B}}_t^{*\mathsf{KP}} := (b_{t,1}^{*\mathsf{KP}}, \ldots, b_{t,n_t^{\mathsf{KP}}}^{*\mathsf{KP}}, b_{t,2n_t^{\mathsf{KP}}+1}^{*\mathsf{KP}}, \ldots, b_{t,3n_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$

$$\text{for } t = 1, \ldots, d^{\mathsf{CP}}, \quad \hat{\mathbb{B}}_t^{\mathsf{CP}} := (b_{t,1}^{\mathsf{CP}}, \ldots, b_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}}, b_{t,3n_t^{\mathsf{CP}}+1}^{\mathsf{CP}}),$$

$$\hat{\mathbb{B}}_t^{*\mathsf{CP}} := (b_{t,1}^{*\mathsf{CP}}, \ldots, b_{t,n_t^{\mathsf{CP}}}^{*\mathsf{CP}}, b_{t,2n_t^{\mathsf{CP}}+1}^{*\mathsf{CP}}, \ldots, b_{t,3n_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$

$$\mathsf{pk} := (1^{\lambda}, \mathsf{param}_{\vec{n}}, \hat{\mathbb{B}}_0, \{\hat{\mathbb{B}}_t^{\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}}, \{\hat{\mathbb{B}}_t^{\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}),$$

$$\mathsf{sk} := (\hat{\mathbb{B}}_0^*, \{\hat{\mathbb{B}}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}}, \{\hat{\mathbb{B}}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})$$

return pk, sk.

[数161]

$$\mathcal{G}_{\mathsf{ob}}{}^{\mathsf{up}}(1^{\lambda},\vec{n}:=((d^{\mathsf{KP}};n_1^{\mathsf{KP}},\ldots,n_{d^{\mathsf{KP}}}^{\mathsf{KP}}),(d^{\mathsf{CP}};n_1^{\mathsf{CP}},\ldots,n_{d^{\mathsf{CP}}}^{\mathsf{CP}})):$$

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

$$N_0:=8,\quad N_t^{\mathsf{KP}}:=3n_t^{\mathsf{KP}}+1\ \text{ for } t=1,\ldots,d^{\mathsf{KP}},$$

$$N_t^{\mathsf{CP}}:=3n_t^{\mathsf{CP}}+1\ \text{ for } t=1,\ldots,d^{\mathsf{CP}},$$

$$\mathsf{param}_{\mathbb{V}_0}:=(q,\mathbb{V}_0,\mathbb{G}_T,\mathbb{A}_0,e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_0,\mathsf{param}_{\mathbb{G}}),$$

$$X_0:=(\chi_{0,i,j})_{i,j}\xleftarrow{\mathsf{U}}GL(N_0,\mathbb{F}_q),\quad (\nu_{0,i,j})_{i,j}:=\psi\cdot(X_0^{\mathrm{T}})^{-1},$$

$$b_{0,i}:=(\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\quad \mathbb{B}_0:=(b_{0,1},\ldots,b_{0,N_0}),$$

$$b_{0,i}^{*}:=(\nu_{0,i,1},\ldots,\nu_{0,i,N_0})_{\mathbb{A}_0},\quad \mathbb{B}_0^{*}:=(b_{0,i}^{*},\ldots,b_{0,N_0}^{*}),$$

for $t=1,\ldots,d^{\mathsf{KP}}$,

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

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

$$b_{t,i}^{\mathsf{KP}}:=(\chi_{t,i,1}^{\mathsf{KP}},\ldots,\chi_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\quad \mathbb{B}_t^{\mathsf{KP}}:=(b_{t,1}^{\mathsf{KP}},\ldots,b_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}}),$$

$$b_{t,i}^{*\mathsf{KP}}:=(\nu_{t,i,1}^{\mathsf{KP}},\ldots,\nu_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\quad \mathbb{B}_t^{*\mathsf{KP}}:=(b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$

for $t=1,\ldots,d^{\mathsf{CP}}$,

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

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

$$b_{t,i}^{\mathsf{CP}}:=(\chi_{t,i,1}^{\mathsf{CP}},\ldots,\chi_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\quad \mathbb{B}_t^{\mathsf{CP}}:=(b_{t,1}^{\mathsf{CP}},\ldots,b_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}}),$$

$$b_{t,i}^{*\mathsf{CP}}:=(\nu_{t,i,1}^{\mathsf{CP}},\ldots,\nu_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\quad \mathbb{B}_t^{*\mathsf{CP}}:=(b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$

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

$$\mathsf{param}_{\vec{n}}:=(\mathsf{param}_{\mathbb{V}_0},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}\}_{t=1,\ldots,d^{\mathsf{CP}}},g_T)$$

$$\mathsf{return}\ (\mathsf{param}_{\vec{n}},\{\mathbb{B}_0,\mathbb{B}_0^{*}\},\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}).$$

また、数１４４に示すＫｅｙＧｅｎアルゴリズムは、数１６２のように書き換えられる。

[数162]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\mathbb{S}^{\mathsf{KP}}:=(M^{\mathsf{KP}},\rho^{\mathsf{KP}}),$$

$$\Gamma^{\mathsf{CP}}:=\{(t,\vec{x}_t^{\mathsf{CP}}:=(x_{t,1}^{\mathsf{CP}},\ldots,x_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}})$$

$$\in\mathbb{F}_q^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})\,\big|\,1\le t\le d^{\mathsf{CP}},x_{t,1}^{\mathsf{CP}}:=1\})$$

$$\vec{f}^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{r^{\mathsf{KP}}},\quad(\vec{s}^{\mathsf{KP}})^{\mathrm{T}}:=(s_1^{\mathsf{KP}},\ldots,s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}}:=M^{\mathsf{KP}}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{KP}}:=\vec{1}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$\delta^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_t^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t^{\mathsf{CP}}}\ \text{ such that }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$(\eta_{0,1},\eta_{0,2})\xleftarrow{\mathsf{U}}\mathbb{F}_q^2,$$

$$k_0^*:=(-s_0^{\mathsf{KP}},\delta^{\mathsf{CP}},0,0,1,\eta_{0,1},\eta_{0,2},0)_{\mathbb{B}_0^*},$$

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

$$\text{if }\rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}}:=(v_{i,1}^{\mathsf{KP}},\ldots,v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}})\in\mathbb{F}_q^{n_t^{\mathsf{KP}}}\setminus\{\vec{0}\}),$$

$$\theta_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{e}_{t,1}^{\mathsf{KP}}+\theta_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0}^{1})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{if }\rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}}),\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0}^{1})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{for }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$k_t^{*\mathsf{CP}}:=(\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}},\overbrace{\vec{\eta}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0}^{1})_{\mathbb{B}_t^{*\mathsf{CP}}},$$

$$\mathsf{return}\ \mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})}:=$$

$$(k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\}_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}}).$$

また、数１５４に示すＥｎｃアルゴリズムは、数１６３のように書き換えられる。

[数163]

$$
\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, m, \Gamma^{\mathsf{KP}} :=\\
&\quad \{(t, \vec{x}_t^{\mathsf{KP}} := (x_{t,1}^{\mathsf{KP}}, \ldots, x_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}) \in \mathbb{F}_q^{n_t^{\mathsf{KP}}} \setminus \{\vec{0}\}) \mid 1 \le t \le d^{\mathsf{KP}}, x_{t,1}^{\mathsf{KP}} := 1\},\\
&\quad \mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}}, \rho^{\mathsf{CP}})):\\
&\qquad \omega^{\mathsf{KP}}, \varphi_0, \varphi_t^{\mathsf{KP}}, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma,\\
&\qquad \vec{f}^{\mathsf{CP}} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{r^{\mathsf{CP}}}, (\vec{s}^{\mathsf{CP}})^{\mathrm{T}} := (s_1^{\mathsf{CP}}, \ldots, s_{L^{\mathsf{CP}}}^{\mathsf{CP}})^{\mathrm{T}} := M^{\mathsf{CP}} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad s_0^{\mathsf{CP}} := \vec{1} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, 0, 0, \zeta, 0, 0, \varphi_0)_{\mathbb{B}_0},\\
&\qquad \text{for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}},\\
&\qquad\quad c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}} \vec{x}_t^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}}, \overbrace{\varphi_t^{\mathsf{KP}}}^{1})_{\mathbb{B}_t^{\mathsf{KP}}},\\
&\qquad \text{for } i = 1, \ldots, L^{\mathsf{CP}},\\
&\qquad\quad \text{if } \rho^{\mathsf{CP}}(i) = (t, \vec{v}_i^{\mathsf{CP}} := (v_{i,1}^{\mathsf{CP}}, \ldots, v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}) \in \mathbb{F}_q^{n_t^{\mathsf{CP}}} \setminus \{\vec{0}\}) (v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}} := 1),\\
&\qquad\qquad \varphi_i^{\mathsf{CP}}, \theta_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\qquad\qquad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{e}_{t,1}^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{\varphi_i^{\mathsf{CP}}}^{1})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad\quad \text{if } \rho^{\mathsf{CP}}(i) = \neg(t, \vec{v}_i^{\mathsf{CP}}), \varphi_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\qquad\qquad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{\varphi_i^{\mathsf{CP}}}^{1})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad c_{d+1} := g_T^{\zeta} m,\\
&\qquad \mathsf{return}\ \mathsf{ct}_{(\Gamma^{\mathsf{KP}}, \mathbb{S}^{\mathsf{CP}})} :=\\
&\qquad\quad (c_0; \Gamma^{\mathsf{KP}}, \{c_t^{\mathsf{KP}}\}_{(t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}}}; \mathbb{S}^{\mathsf{CP}}, c_1^{\mathsf{CP}}, \ldots, c_{L^{\mathsf{CP}}}^{\mathsf{CP}}; c_{d+1}).
\end{aligned}
$$

なお、数１５９に示すＤｅｃアルゴリズムには変更はない。

[0087] また、上記説明では、（Ｓ１０１）でN_0に８を設定した。しかし、N_0は８ではなく、３以上の整数であればよい。N_0が３であると、基底B_0と基底

B^{*}_{0}とが２次元になる。N_0が３の場合、ＫｅｙＧｅｎアルゴリズムにおいて、$k^{*}_{0}:=(-s_0^{KP}, \delta^{CP}, 1))_{B*0}$とし、Ｅｎｃアルゴリズムにおいて、$c_0:=(\omega^{KP}, -s_0^{CP}, \zeta)_{B0}$とすればよい。ここで、Ｂ＊０は$B^{*}_{0}$のことであり、Ｂ０は$B_0$のことである。

[0088] また、上記説明では、ＫｅｙＧｅｎアルゴリズムにおいて、$k^{*}_{0}:=(-s_0, \delta^{CP}, 0, 0, 1, \eta_{0,1}, \eta_{0,2}, 0)_{B*0}$とした。しかし、暗号化装置２００が知りえる所定の値κを用いて、$k^{*}_{0}:=(-s_0, \delta^{CP}, 0, 0, \kappa, \eta_{0,1}, \eta_{0,2}, 0)_{B*0}$としてもよい。ここで、Ｂ＊０は$B^{*}_{0}$のことであり、Ｂ０は$B_0$のことである。この場合、Ｄｅｃアルゴリズムで計算されるＫ：＝$g^{\zeta\kappa_T}$となるため、Ｅｎｃアルゴリズムにおいて、$c_{d+1}:=g^{\zeta\kappa_T}$ｍとすればよい。

[0089] また、上記説明では、$v_{i,ntCP}^{CP}$（ここでｎｔＣＰはn_t^{CP}のことである）の値について特に限定しなかった。しかし、安全性の証明の観点から、$v_{i,ntCP}^{CP}:=1$である限定としてもよい。

[0090] また、安全性の証明の観点から、ｉ＝１，．．．，L^{KP}の各整数ｉについてのρ^{KP}（ｉ）は、それぞれ異なる識別情報ｔについての肯定形の組（ｔ，$\vec{v}_i^{KP}$）又は否定形の組¬（ｔ，$\vec{v}_i^{KP}$）であると限定してもよい。

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

同様に、ｉ＝１，．．．，L^{CP}の各整数ｉについてのρ^{CP}（ｉ）は、それぞれ異なる識別情報ｔについての肯定形の組（ｔ，$\vec{v}_i^{CP}$）又は否定形の組¬（ｔ，$\vec{v}_i^{CP}$）であると限定してもよい。

言い替えると、ρ^{CP}（ｉ）＝（ｔ，$\vec{v}_i^{CP}$）又はρ^{CP}（ｉ）＝¬（ｔ，$\vec{v}_i^{CP}$）である場合に、関数ρ$^{\sim CP}$を、ρ$^{\sim CP}$（ｉ）＝ｔである｛１，．．．，Ｌ｝→｛１，．．，d^{CP}｝の写像であるとする。この場合、ρ$^{\sim CP}$が単射であ

ると限定してもよい。なお、ρ^{CP}（ｉ）は、上述したアクセスストラクチャS^{CP}：＝（M^{CP}，ρ^{CP}（ｉ））のρ^{CP}（ｉ）である。

[0091] 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。

[0092] また、上記説明では、スパンプログラム$M\hat{}$は、入力列δによって行列$M\hat{}$から得られる行列M_{δ}の行を線形結合して$1^{\rightarrow}$が得られる場合に限り、入力列δを受理するとした。しかし、スパンプログラム$M\hat{}$は、$1^{\rightarrow}$ではなく、他のベクトル$h^{\rightarrow}$が得られる場合に限り、入力列δを受理するとしてもよい。

この場合、ＫｅｙＧｅｎアルゴリズムにおいて、s_0^{KP}：＝$1^{\rightarrow}\cdot(f^{\rightarrow KP})^{T}$ではなく、$s_0$：＝$h^{\rightarrow KP}\cdot(f^{\rightarrow KP})^{T}$とすればよい。同様に、Ｅｎｃアルゴリズムにおいて、s_0^{CP}：＝$1^{\rightarrow}\cdot(f^{\rightarrow CP})^{T}$ではなく、$s_0$：＝$h^{\rightarrow CP}\cdot(f^{\rightarrow CP})^{T}$とすればよい。

[0093] 実施の形態２．

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。

[0094] 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１６４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164]

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

ここで、
$\mathbb{Z}$ ：整数
M ：合成数
である。

[0095] 例えば、実施の形態１で説明したＵｎｉｆｉｅｄ－Ｐｏｌｉｃｙ関数型暗号を、環Ｒを係数とする加群において実現すると数１６５から数１６９のようになる。

[数165]

$$\mathcal{G}_{\mathsf{ob}}{}^{\mathsf{up}}(1^{\lambda},\vec{n}:=((d^{\mathsf{KP}};n_t^{\mathsf{KP}},u_t^{\mathsf{KP}},w_t^{\mathsf{KP}},z_t^{\mathsf{KP}}\left(t=1,...,d^{\mathsf{KP}}\right)),$$
$$(d^{\mathsf{CP}};n_t^{\mathsf{CP}},u_t^{\mathsf{CP}},w_t^{\mathsf{CP}},z_t^{\mathsf{CP}}\left(t=1,...,d^{\mathsf{CP}}\right))):$$
$$\mathsf{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{\mathsf{R}}\mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),\quad \psi\xleftarrow{\mathsf{U}}\mathbb{R}^{\mathsf{X}},$$
$$N_0:=2+u_0+1+w_0+z_0,$$
$$N_t^{\mathsf{KP}}:=n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}}\ \text{ for }\ t=1,\ldots,d^{\mathsf{KP}},$$
$$N_t^{\mathsf{CP}}:=n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}}\ \text{ for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\mathsf{param}_{\mathbb{V}_0}:=(q,\mathbb{V}_0,\mathbb{G}_T,\mathbb{A}_0,e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_0,\mathsf{param}_{\mathbb{G}}),$$
$$X_0:=(\chi_{0,i,j})_{i,j}\xleftarrow{\mathsf{U}}GL(N_0,\mathbb{R}),\quad (\nu_{0,i,j})_{i,j}:=\psi\cdot(X_0^{\mathrm{T}})^{-1},$$
$$b_{0,i}:=(\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0:=(b_{0,1},\ldots,b_{0,N_0}),$$
$$b_{0,i}^*:=(\nu_{0,i,1},\ldots,\nu_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0^*:=(b_{0,i}^*,\ldots,b_{0,N_0}^*),$$
$$\text{for } t=1,\ldots,d^{\mathsf{KP}},$$
$$\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}:=(q,\mathbb{V}_t^{\mathsf{KP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{KP}},e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{KP}},\mathsf{param}_{\mathbb{G}}),$$
$$X_t^{\mathsf{KP}}:=(\chi_{t,i,j}^{\mathsf{KP}})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t^{\mathsf{KP}},\mathbb{F}_q),\quad (\nu_{t,i,j}^{\mathsf{KP}})_{i,j}:=\psi\cdot((X_t^{\mathsf{KP}})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{\mathsf{KP}}:=(\chi_{t,i,1}^{\mathsf{KP}},\ldots,\chi_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{\mathsf{KP}}:=(b_{t,1}^{\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{\mathsf{KP}}),$$
$$b_{t,i}^{*\mathsf{KP}}:=(\nu_{t,i,1}^{\mathsf{KP}},\ldots,\nu_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{*\mathsf{KP}}:=(b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$
$$\text{for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}:=(q,\mathbb{V}_t^{\mathsf{CP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{CP}},e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{CP}},\mathsf{param}_{\mathbb{G}}),$$
$$X_t^{\mathsf{CP}}:=(\chi_{t,i,j}^{\mathsf{CP}})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t^{\mathsf{CP}},\mathbb{F}_q),\quad (\nu_{t,i,j}^{\mathsf{CP}})_{i,j}:=\psi\cdot((X_t^{\mathsf{CP}})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{\mathsf{CP}}:=(\chi_{t,i,1}^{\mathsf{CP}},\ldots,\chi_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{\mathsf{CP}}:=(b_{t,1}^{\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{\mathsf{CP}}),$$
$$b_{t,i}^{*\mathsf{CP}}:=(\nu_{t,i,1}^{\mathsf{CP}},\ldots,\nu_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{*\mathsf{CP}}:=(b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$
$$g_T:=e(g,g)^{\psi},$$
$$\mathsf{param}_{\vec{n}}:=(\mathsf{param}_{\mathbb{V}_0},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}\}_{t=1,\ldots,d^{\mathsf{CP}}},g_T)$$
$$\text{return }(\mathsf{param}_{\vec{n}},\{\mathbb{B}_0,\mathbb{B}_0^*\},\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}).$$

[数166]

$$\mathsf{Setup}(1^{\lambda},\vec{n} := ((d^{\mathsf{KP}};n_t^{\mathsf{KP}},u_t^{\mathsf{KP}},w_t^{\mathsf{KP}},z_t^{\mathsf{KP}}\left(t=1,...,d^{\mathsf{KP}}\right)),$$
$$(d^{\mathsf{CP}};n_t^{\mathsf{CP}},u_t^{\mathsf{CP}},w_t^{\mathsf{CP}},z_t^{\mathsf{CP}}\left(t=1,...,d^{\mathsf{CP}}\right))):$$
$$(\mathsf{param}_{\vec{n}},\mathbb{B}_0,\mathbb{B}_0^*,\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},$$
$$\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}),$$
$$\hat{\mathbb{B}}_0 := (b_{0,1}^*,b_{0,2}^*,b_{0,2+u_0+1}^*,b_{0,2+u_0+1+w_0+1}^*,\ldots,b_{0,2+u_0+1+w_0+z_0}^*),$$
$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*,b_{0,2}^*,b_{0,2+u_0+1}^*,b_{0,2+u_0+1+1}^*,\ldots,b_{0,2+u_0+1+w_0}^*),$$
$$\text{for } t=1,\ldots,d^{\mathsf{KP}},$$
$$\hat{\mathbb{B}}_t^{\mathsf{KP}} := (b_{t,1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}},b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}}}^{\mathsf{KP}}),$$
$$\hat{\mathbb{B}}_t^{*\mathsf{KP}} := (b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{*\mathsf{KP}},b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$
$$\text{for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\hat{\mathbb{B}}_t^{\mathsf{CP}} := (b_{t,1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}},b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}}}^{\mathsf{CP}}),$$
$$\hat{\mathbb{B}}_t^{*\mathsf{CP}} := (b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{*\mathsf{CP}},b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$
$$\mathsf{pk} := (1^{\lambda},\mathsf{param}_{\vec{n}},\hat{\mathbb{B}}_0,\{\hat{\mathbb{B}}_t^{\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}),$$
$$\mathsf{sk} := (\hat{\mathbb{B}}_0^*,\{\hat{\mathbb{B}}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})$$
$$\text{return pk, sk.}$$

[数167]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\mathbb{S}^{\mathsf{KP}}:=(M^{\mathsf{KP}},\rho^{\mathsf{KP}}),$$

$$\Gamma^{\mathsf{CP}}:=\{(t,\vec{x}_t^{\mathsf{CP}}:=(x_{t,1}^{\mathsf{CP}},\ldots,x_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}})\in\mathbb{R}^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})$$

$$\left|1\le t\le d^{\mathsf{CP}},x_{t,1}^{\mathsf{CP}}:=1\right\})$$

$$\vec{f}^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{r^{\mathsf{KP}}},\quad(\vec{s}^{\mathsf{KP}})^{\mathrm{T}}:=(s_1^{\mathsf{KP}},\ldots,s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}}:=M^{\mathsf{KP}}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{KP}}:=\vec{1}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$\delta^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{R},\quad\vec{\eta}_t^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t^{\mathsf{CP}}}\ \text{such that}\ (t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$\vec{\eta}_0\xleftarrow{\mathsf{U}}\mathbb{R}^{w_0},$$

$$k_0^*:=(-s_0^{\mathsf{KP}},\delta^{\mathsf{CP}},\overbrace{0^{u_0}}^{u_0},1,\overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0},\overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

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

$$\text{if } \rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}}:=(v_{i,1}^{\mathsf{KP}},\ldots,v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}})\in\mathbb{R}^{n_t^{\mathsf{KP}}}\setminus\{\vec{0}\}),$$

$$\theta_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R},\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{e}_{t,1}^{\mathsf{KP}}+\theta_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{if } \rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}}),\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{for } (t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$k_t^{*\mathsf{CP}}:=(\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}},\overbrace{\vec{\eta}_t^{\mathsf{CP}}}^{w_t^{\mathsf{CP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{*\mathsf{CP}}},$$

$$\mathsf{return}\ \mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})}:=$$

$$(k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\}_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}}).$$

[数168]

$$\mathsf{Enc}(\mathsf{pk}, m, \Gamma^{\mathsf{KP}} :=$$

$$\{(t, \vec{x}_t^{\mathsf{KP}} := (x_{t,1}^{\mathsf{KP}}, \ldots, x_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}) \in \mathbb{R}^{n_t^{\mathsf{KP}}} \setminus \{\vec{0}\}) \mid 1 \le t \le d^{\mathsf{KP}}, x_{t,1}^{\mathsf{KP}} := 1\},$$

$$\mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}}, \rho^{\mathsf{CP}})):$$

$$\omega^{\mathsf{KP}}, \zeta \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{R}^{z_0},\ \vec{\varphi}_t^{\mathsf{KP}} \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t^{\mathsf{KP}}} \text{ for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma,$$

$$\vec{f}^{\mathsf{CP}} \xleftarrow{\mathsf{R}} \mathbb{R}^{r^{\mathsf{CP}}}, (\vec{s}^{\mathsf{CP}})^{\mathrm{T}} := (s_1^{\mathsf{CP}}, \ldots, s_{L^{\mathsf{CP}}}^{\mathsf{CP}})^{\mathrm{T}} := M^{\mathsf{CP}} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{CP}} := \vec{1} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},$$

$$c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\varphi_{0,1}, \ldots, \varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0},$$

$$\text{for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}},$$

$$c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}} \vec{x}_t^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}}, \overbrace{0^{w_t^{\mathsf{KP}}}}^{w_t^{\mathsf{KP}}}, \overbrace{\vec{\varphi}_t^{\mathsf{KP}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{\mathsf{KP}}}$$

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

$$\text{if } \rho^{\mathsf{CP}}(i) = (t, \vec{v}_i^{\mathsf{CP}} := (v_{i,1}^{\mathsf{CP}}, \ldots, v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}) \in \mathbb{R}^{n_t^{\mathsf{CP}}} \setminus \{\vec{0}\}),$$

$$\theta_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t^{\mathsf{CP}}},$$

$$c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{e}_{t,1}^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_i^{\mathsf{CP}}},$$

$$\text{if } \rho^{\mathsf{CP}}(i) = \neg(t, \vec{v}_i^{\mathsf{CP}}),\ \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t^{\mathsf{CP}}},$$

$$c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_i^{\mathsf{CP}}},$$

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

$$\text{return } \mathsf{ct}_{(\Gamma^{\mathsf{KP}}, \mathbb{S}^{\mathsf{CP}})} :=$$

$$(c_0; \Gamma^{\mathsf{KP}}, \{c_t^{\mathsf{KP}}\}_{(t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}}}; \mathbb{S}^{\mathsf{CP}}, c_1^{\mathsf{CP}}, \ldots, c_{L^{\mathsf{CP}}}^{\mathsf{CP}}; c_{d+1}).$$

[数169]

$$
\begin{aligned}
&\mathrm{Dec}(\mathrm{pk},\\
&\quad \mathrm{sk}_{(\mathbb{S}^{\mathrm{KP}},\Gamma^{\mathrm{CP}})} := (k_0^*;\mathbb{S}^{\mathrm{KP}},k_1^{*\mathrm{KP}},\ldots,k_{L^{\mathrm{KP}}}^{*\mathrm{KP}};\Gamma^{\mathrm{CP}},\{k_t^{*\mathrm{CP}}\})_{(t,\vec{x}_t^{\mathrm{CP}})\in\Gamma^{\mathrm{CP}}}),\\
&\quad \mathrm{ct}_{(\Gamma^{\mathrm{KP}},\mathbb{S}^{\mathrm{CP}})} := (c_0;\Gamma^{\mathrm{KP}},\{c_t^{\mathrm{KP}}\}_{(t,\vec{x}_t^{\mathrm{KP}})\in\Gamma^{\mathrm{KP}}};\mathbb{S}^{\mathrm{CP}},c_1^{\mathrm{CP}},\ldots,c_{L^{\mathrm{CP}}}^{\mathrm{CP}};c_{d+1})):\\
&\quad \text{If } \mathbb{S}^{\mathrm{KP}} := (M^{\mathrm{KP}},\rho^{\mathrm{KP}}) \text{ accepts } \Gamma^{\mathrm{KP}} := \{(t,\vec{x}_t^{\mathrm{KP}})\}\\
&\quad \text{and } \mathbb{S}^{\mathrm{CP}} := (M^{\mathrm{CP}},\rho^{\mathrm{CP}}) \text{ accepts } \Gamma^{\mathrm{CP}} := \{(t,\vec{x}_t^{\mathrm{CP}})\},\\
&\quad \text{then compute } (I^{\mathrm{KP}},\{\alpha_i^{\mathrm{KP}}\}_{i\in I^{\mathrm{KP}}}) \text{ and } (I^{\mathrm{CP}},\{\alpha_i^{\mathrm{CP}}\}_{i\in I^{\mathrm{CP}}}) \text{ such that}\\
&\quad\quad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{\mathrm{KP}} M_i^{\mathrm{KP}}, \text{ where } M_i^{\mathrm{KP}} \text{ is the } i-\text{th row of } M^{\mathrm{KP}}, \text{and}\\
&\quad\quad I^{\mathrm{KP}} \subseteq \{i\in\{1,\ldots,L^{\mathrm{KP}}\}\\
&\quad\quad\quad \Big|[\rho^{\mathrm{KP}}(i)=(t,\vec{v}_i^{\mathrm{KP}})\wedge(t,\vec{x}_t^{\mathrm{KP}})\in\Gamma^{\mathrm{KP}}\wedge\vec{v}_i^{\mathrm{KP}}\cdot\vec{x}_t^{\mathrm{KP}}=0]\\
&\quad\quad\quad \vee[\rho^{\mathrm{KP}}(i)=\neg(t,\vec{v}_i^{\mathrm{KP}})\wedge(t,\vec{x}_t^{\mathrm{KP}})\in\Gamma^{\mathrm{KP}}\wedge\vec{v}_i^{\mathrm{KP}}\cdot\vec{x}_t^{\mathrm{KP}}\neq 0]\}, \text{and}\\
&\quad\quad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{\mathrm{CP}} M_i^{\mathrm{CP}}, \text{ where } M_i^{\mathrm{CP}} \text{ is the } i-\text{th row of } M^{\mathrm{CP}}, \text{and}\\
&\quad\quad I^{\mathrm{CP}} \subseteq \{i\in\{1,\ldots,L^{\mathrm{CP}}\}\\
&\quad\quad\quad \Big|[\rho^{\mathrm{CP}}(i)=(t,\vec{v}_i^{\mathrm{CP}})\wedge(t,\vec{x}_t^{\mathrm{CP}})\in\Gamma^{\mathrm{CP}}\wedge\vec{v}_i^{\mathrm{CP}}\cdot\vec{x}_t^{\mathrm{CP}}=0]\\
&\quad\quad\quad \vee[\rho^{\mathrm{CP}}(i)=\neg(t,\vec{v}_i^{\mathrm{CP}})\wedge(t,\vec{x}_t^{\mathrm{CP}})\in\Gamma^{\mathrm{CP}}\wedge\vec{v}_i^{\mathrm{CP}}\cdot\vec{x}_t^{\mathrm{CP}}\neq 0]\},\\
&\quad\quad K := e(c_0,k_0^*)\cdot\\
&\quad\quad\quad \prod_{i\in I^{\mathrm{KP}}\wedge\rho^{\mathrm{KP}}(i)=(t,\vec{v}_i^{\mathrm{KP}})} e(c_t^{\mathrm{KP}},k_i^{*\mathrm{KP}})^{\alpha_i^{\mathrm{KP}}}\cdot\\
&\quad\quad\quad \prod_{i\in I^{\mathrm{KP}}\wedge\rho^{\mathrm{KP}}(i)=\neg(t,\vec{v}_i^{\mathrm{KP}})} e(c_t^{\mathrm{KP}},k_i^{*\mathrm{KP}})^{\alpha_i^{\mathrm{KP}}/(\vec{v}_i^{\mathrm{KP}}\cdot\vec{x}_t^{\mathrm{KP}})}\cdot\\
&\quad\quad\quad \prod_{i\in I^{\mathrm{CP}}\wedge\rho^{\mathrm{CP}}(i)=(t,\vec{v}_i^{\mathrm{CP}})} e(c_t^{\mathrm{CP}},k_i^{*\mathrm{CP}})^{\alpha_i^{\mathrm{CP}}}\cdot\\
&\quad\quad\quad \prod_{i\in I^{\mathrm{CP}}\wedge\rho^{\mathrm{CP}}(i)=\neg(t,\vec{v}_i^{\mathrm{CP}})} e(c_t^{\mathrm{CP}},k_i^{*\mathrm{CP}})^{\alpha_i^{\mathrm{CP}}/(\vec{v}_i^{\mathrm{CP}}\cdot\vec{x}_t^{\mathrm{CP}})},\\
&\quad\quad \text{return } m' := c_{d+1}/K.
\end{aligned}
$$

[0096] また、上記説明における暗号処理は、権限の委譲を行うことも可能である。権限の委譲とは、復号鍵を有する者がその復号鍵よりも権限の弱い下位の復号鍵を生成することである。ここで、権限が弱いとは、復号できる暗号化データが限定されるという意味である。

例えば、第１階層目（最上位）においては、ｔ＝１の基底$Ｂ_t$と基底$Ｂ^*_t$とを用い、第２階層目においては、ｔ＝１，２の基底$Ｂ_t$と基底$Ｂ^*_t$とを用い、・・・、第ｋ階層目においては、ｔ－１，．．．，ｋの基底$Ｂ_t$と基底$Ｂ^*_t$とを用いる。用いる基底$Ｂ_t$と基底$Ｂ^*_t$とが増える分、属性情報が多く設定されることになる。したがって、より復号鍵の権限が限定されることになる。

[0097] 次に、実施の形態における暗号処理システム１０（鍵生成装置１００、暗号化装置２００、復号装置３００）のハードウェア構成について説明する。

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

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

[0098] 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。

[0099] 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。

[0100] 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」、「情報入力部１３０」、「復号鍵生成部１４０」、「鍵配布部１５０」、「公開パラメータ取得部２１０」、「情報入力部２２０」、「暗号化データ生成部２３０」、「データ送信部２４０」、「復号鍵取得部３１０」、「データ受信部３２０」、「スパンプログラム計算部３３０」、「補完係数計算部３４０」、「ペアリング演算部３５０」、「メッセージ計算部３６０」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、上記の説明において「公開パラメータｐｋ」、「マスター鍵ｓｋ」、「暗号化データｃｔ$_{(\Gamma_{KP}, S_{CP})}$」、「復号鍵ｓｋ$_{(S_{KP}, \Gamma_{CP})}$」、「アクセスストラクチャS_{KP}，S_{CP}」、「属性の集合Γ_{KP}，Γ_{CP}」、「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。

[0101] 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

[0102] 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、１３１　ＫＰ情報入力部、１３２　ＣＰ情報入力部、１４０　復号鍵生成部、１４１　ｆベクトル生成部、１４２　ｓベクトル生成部、１４３　乱数生成部、１４４　主復号鍵生成部、１４５　ＫＰ復号鍵生成部、１４６　ＣＰ復号鍵生成部、１５０　鍵配布部、２００　暗号化装置、２１０　公開パラメータ取得部、２２０　情報入力部、２２１　ＫＰ情報入力部、２２２　ＣＰ情報入力部、２２３　メッセージ入力部、２３０　暗号化データ生成部、２３１　ｆベクトル生成部、２３２　ｓベクトル生成部、２３３　乱数生成部、２３４　主暗号

化データ生成部、２３５　ＫＰ暗号化データ生成部、２３６　ＣＰ暗号化データ生成部、２３７　メッセージ暗号化データ生成部、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　スパンプログラム計算部、３３１　ＫＰスパンプログラム計算部、３３２　ＣＰスパンプログラム計算部、３４０　補完係数計算部、３４１　ＫＰ補完係数計算部、３４２　ＣＰ補完係数計算部、３５０　ペアリング演算部、３６０　メッセージ計算部。

請求の範囲

［請求項1］ 鍵生成装置と暗号化装置と復号装置とを備え、基底B_0及び基底B_0^*と、$t=1,\ldots,d^{KP}$（d^{KP}は１以上の整数）の各整数ｔについての基底B_t^{KP}及び基底$B^*_t{}^{KP}$と、$t=1,\ldots,d^{CP}$（d^{CP}は１以上の整数）の各整数ｔについての基底B_t^{CP}及び基底$B^*_t{}^{CP}$とを用いて暗号処理を実行する暗号処理システムであり、

前記鍵生成装置は、

$i=1,\ldots,L^{KP}$（L^{KP}は１以上の整数）の各整数ｉについての変数$\rho^{KP}(i)$であって、識別情報ｔ（$t=1,\ldots,d^{KP}$のいずれかの整数）と、属性ベクトル$\vec{v}_i^{KP}:=(v_{i,i'}{}^{KP})$（$i'=1,\ldots,n_t^{KP}$，$n_t^{KP}$は１以上の整数）との肯定形の組（ｔ，$\vec{v}_i^{KP}$）又は否定形の組￢（ｔ，$\vec{v}_i^{KP}$）のいずれかである変数$\rho^{KP}(i)$と、$L^{KP}$行$r^{KP}$列（$r^{KP}$は１以上の整数）の所定の行列$M^{KP}$とを入力する第１ＫＰ情報入力部と、

$t=1,\ldots,d^{CP}$の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}_t^{CP}:=(x_{t,i'}{}^{CP})$（$i'=1,\ldots,n_t^{CP}$，$n_t^{CP}$は１以上の整数）とを有する属性集合$\Gamma^{CP}$を入力する第１ＣＰ情報入力部と、

基底B^*_0の基底ベクトル$b^*_{0,p}$（ｐは所定の値）の係数として値$-s_0^{KP}$（$s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$，$\vec{h}^{KP}$及び$\vec{f}^{KP}$は$r^{KP}$個の要素を有するベクトル）を設定し、基底ベクトル$b^*_{0,p'}$（ｐ’は前記ｐとは異なる所定の値）の係数として乱数δ^{CP}を設定し、基底ベクトル$b^*_{0,q}$（ｑは前記ｐ及び前記ｐ’とは異なる所定の値）の係数として所定の値κを設定して要素k^*_0を生成する主復号鍵生成部と、

前記$\vec{f}^{KP}$と、前記第１ＫＰ情報入力部が入力した行列M^{KP}に基づき生成される列ベクトル$(\vec{s}^{KP})^T:=(s_1^{KP},\ldots,s_i^{KP})^T:=M^{KP}\cdot(\vec{f}^{KP})^T$（$i=L^{KP}$）と、乱数$\theta_i^{KP}$（$i=1,\ldots$

．，Ｌ^{KP}）とに基づき、ｉ＝１，．．．，Ｌ^{KP}の各整数ｉについての要素ｋ＊$_{i}^{KP}$を生成するＫＰ復号鍵生成部であって、ｉ＝１，．．．，Ｌ^{KP}の各整数ｉについて、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，ｖ→$_{i}^{KP}$）である場合には、その組の識別情報ｔが示す基底Ｂ＊$_{t}^{KP}$の基底ベクトルｂ＊$_{t,1}^{KP}$の係数としてｓ$_{i}^{KP}$＋θ$_{i}^{KP}$ｖ$_{i,1}^{KP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，ｎ$_{t}^{KP}$の各整数ｉ’とが示す基底ベクトルｂ＊$_{t,i'}^{KP}$の係数としてθ$_{i}^{KP}$ｖ$_{i,i'}^{KP}$を設定して要素ｋ＊$_{i}^{KP}$を生成し、変数ρ^{KP}（ｉ）が否定形の組￢（ｔ，ｖ→$_{i}^{KP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，ｎ$_{t}^{KP}$の各整数ｉ’とが示す基底ベクトルｂ＊$_{t,i'}^{KP}$の係数としてｓ$_{i}^{KP}$ｖ$_{i,i'}^{KP}$を設定して要素ｋ＊$_{i}^{KP}$を生成するＫＰ復号鍵生成部と、

前記第１ＣＰ情報入力部が入力した属性集合Γ^{CP}に含まれる各識別情報ｔについての要素ｋ＊$_{t}^{CP}$を生成するＣＰ復号鍵生成部であって、基底Ｂ＊$_{t}^{CP}$の基底ベクトルｂ＊$_{t,i'}^{CP}$（ｉ’＝１，．．．，ｎ$_{t}^{CP}$）の係数として前記乱数δ^{CP}倍したｘ$_{t,i'}^{CP}$を設定して要素ｋ＊$_{t}^{CP}$を生成するＣＰ復号鍵生成部と

を備え、

前記暗号化装置は、

ｔ＝１，．．．，ｄ^{KP}の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトルｘ→$_{t}^{KP}$：＝（ｘ$_{t,i'}^{KP}$）（ｉ’＝１，．．．，ｎ$_{t}^{KP}$）とを有する属性集合Γ^{KP}を入力する第２ＫＰ情報入力部と、

ｉ＝１，．．．，Ｌ^{CP}（Ｌ^{CP}は１以上の整数）の各整数ｉについての変数ρ^{CP}（ｉ）であって、識別情報ｔ（ｔ＝１，．．．，ｄ^{CP}のいずれかの整数）と、属性ベクトルｖ→$_{i}^{CP}$：＝（ｖ$_{i,i'}^{CP}$）（ｉ’＝１，．．．，ｎ$_{t}^{CP}$）との肯定形の組（ｔ，ｖ→$_{i}^{CP}$）又は否定形の組￢（ｔ，ｖ→$_{i}^{CP}$）のいずれかである変数ρ^{CP}（ｉ）と、Ｌ^{CP}行

r^{CP}列（r^{CP}は１以上の整数）の所定の行列M^{CP}とを入力する第２ＣＰ情報入力部と、

基底B_0の基底ベクトル$b_{0,p}$の係数として乱数ω^{KP}を設定し、基底ベクトル$b_{0,p'}$の係数として値$-s_0^{CP}$（$s_0^{CP}:=h^{\rightarrow CP}\cdot(f^{\rightarrow CP})^T$，$h^{\rightarrow CP}$及び$f^{\rightarrow CP}$は$r^{CP}$個の要素を有するベクトル）を設定し、基底ベクトル$b_{0,q}$の係数として乱数$\zeta$を設定して要素$c_0$を生成する主暗号化データ生成部と、

前記第２ＫＰ情報入力部が入力した属性集合Γ^{KP}に含まれる各識別情報ｔについての要素c_t^{KP}を生成するＫＰ暗号化データ生成部であって、基底B_t^{KP}の基底ベクトル$b_{t,i',KP}$（$i'=1,\ldots,n_t$）の係数として前記乱数ω^{KP}倍した$x_{t,i',KP}$を設定して要素c_t^{KP}を生成するＫＰ暗号化データ生成部と、

前記$f^{\rightarrow CP}$と、前記第２ＣＰ情報入力部が入力した行列M^{CP}とに基づき生成される列ベクトル$(s^{\rightarrow CP})^T:=(s_1^{CP},\ldots,s_i^{CP})^T:=M^{CP}\cdot(f^{\rightarrow CP})^T$（$i=L^{CP}$）と、乱数$\theta_i^{CP}$（$i=1,\ldots,L^{CP}$）とに基づき、$i=1,\ldots,L^{CP}$の各整数ｉについての要素$c_i^{CP}$を生成するＣＰ暗号化データ生成部であって、$i=1,\ldots,L^{CP}$の各整数ｉについて、変数$\rho^{CP}$（ｉ）が肯定形の組（ｔ，$v^{\rightarrow}{}_i^{CP}$）である場合には、その組の識別情報ｔが示す基底$B_t^{CP}$の基底ベクトル$b_{t,1}^{CP}$の係数として$s_i^{CP}+\theta_i^{CP}v_{i,1}^{CP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，n_t^{CP}の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$\theta_i^{CP}v_{i,i',CP}$を設定して要素c_i^{CP}を生成し、変数ρ^{CP}（ｉ）が否定形の組¬（ｔ，$v^{\rightarrow}{}_i^{CP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，n_t^{CP}の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$s_i^{CP}v_{i,i',CP}$を設定して要素c_i^{CP}を生成するＣＰ暗号化データ生成部と

を備え、

前記復号装置は、

前記主暗号化データ生成部が生成した要素c_0と、前記ＫＰ暗号化データ生成部が生成した要素c_t^{KP}と、前記ＣＰ暗号化データ生成部が生成した要素c_i^{CP}と、前記属性集合Γ^{KP}と、前記変数$\rho^{CP}(i)$とを含む暗号化データ$ct_{(\Gamma KP, SCP)}$を取得するデータ取得部と、

前記主復号鍵生成部が生成した要素k^*_0と、前記ＫＰ復号鍵生成部が生成した要素$k^*_i{}^{KP}$と、前記ＣＰ復号鍵生成部が生成した要素$k^*_t{}^{CP}$と、前記変数$\rho^{KP}(i)$と、前記属性集合Γ^{CP}とを含む復号鍵$sk_{(SKP, \Gamma CP)}$を取得する復号鍵取得部と、

前記データ取得部が取得した暗号化データ$ct_{(\Gamma KP, SCP)}$に含まれる属性集合Γ^{KP}と、前記復号鍵取得部が取得した復号鍵$sk_{(SKP, \Gamma CP)}$に含まれる変数$\rho^{KP}(i)$とに基づき、$i=1,\ldots,L^{KP}$の各整数iのうち、変数$\rho^{KP}(i)$が肯定形の組$(t, \vec{v}_i^{KP})$であり、かつ、その組の$\vec{v}_i^{KP}$と、その組の識別情報tが示すΓ^{KP}に含まれる$\vec{x}_t^{KP}$との内積が０となるiと、変数$\rho^{KP}(i)$が否定形の組$\neg(t, \vec{v}_i^{KP})$であり、かつ、その組の$\vec{v}_i^{KP}$と、その組の識別情報tが示すΓ^{KP}に含まれる$\vec{x}_t^{KP}$との内積が０とならないiとの集合I^{KP}を特定するとともに、特定した集合I^{KP}に含まれるiについて、$\alpha_i^{KP}M_i^{KP}$を合計した場合に前記$h\rightarrow^{KP}$となる補完係数α_i^{KP}を計算するＫＰ補完係数計算部と、

前記暗号化データ$ct_{(\Gamma KP, SCP)}$に含まれる$i=1,\ldots,L^{CP}$の各整数iについての変数$\rho^{CP}(i)$と、前記復号鍵$sk_{(SKP, \Gamma CP)}$に含まれる属性集合Γ^{CP}とに基づき、$i=1,\ldots,L^{CP}$の各整数iのうち、変数$\rho^{CP}(i)$が肯定形の組$(t, \vec{v}_i^{CP})$であり、かつ、その組の$\vec{v}_i^{CP}$と、その組の識別情報tが示すΓ^{CP}に含まれる$\vec{x}_t^{CP}$との内積が０となるiと、変数$\rho^{CP}(i)$が否定形の組$\neg(t, \vec{v}_i^{CP})$であり、かつ、その組の$\vec{v}_i^{CP}$と、その組の識別

情報ｔが示すΓ^{CP}に含まれるｘ$\vec{}_{t}^{CP}$との内積が０とならないｉとの集合Ｉ^{CP}を特定するとともに、特定した集合Ｉ^{CP}に含まれるｉについて、$\alpha_i^{CP}M_i^{CP}$を合計した場合に前記ｈ→^{CP}となる補完係数α_i^{CP}を計算するＣＰ補完係数計算部と、

前記暗号化データｃｔ$_{(\Gamma KP, SCP)}$に含まれる要素ｃ$_0$と要素ｃ$_t^{KP}$と要素ｃ$_i^{CP}$と、前記復号鍵ｓｋ$_{(SKP, \Gamma CP)}$に含まれる要素ｋ＊$_0$と要素ｋ＊$_i^{KP}$と要素ｋ＊$_t^{CP}$とについて、前記ＫＰ補完係数計算部が特定した集合Ｉ^{KP}と、前記ＫＰ

補完係数計算部が計算した補完係数α_i^{KP}と、前記ＣＰ補完係数計算部が特定した集合Ｉ^{CP}と、前記ＣＰ補完係数計算部が計算した補完係数α_i^{CP}とに基づき、数１に示すペアリング演算を行い値Ｋを計算するペアリング演算部と

を備えることを特徴とする暗号処理システム。

[数1]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

[請求項2] 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＝１，２，．．．，２＋ｕ$_0$，２＋ｕ$_0$＋１，．．．，２＋ｕ$_0$＋１＋ｗ$_0$，．．．，２＋ｕ$_0$＋１＋ｚ$_0$）を有する基底Ｂ$_0$と、

少なくとも基底ベクトルｂ＊$_{0,i}$（ｉ＝１，２，．．．，２＋ｕ$_0$，２＋ｕ$_0$＋１，．．．，２＋ｕ$_0$＋１＋ｗ$_0$，．．．，２＋ｕ$_0$＋１＋

z_0）を有する基底B^*_0と、

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

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

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

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

を用いて暗号処理を実行し、

前記鍵生成装置では、

前記主復号鍵生成部は、乱数δ^{CP}，$\eta_{0,i}$（$i=1,\ldots,w_0$）と所定の値κとに基づき数２に示す要素k^*_0を生成し、

前記ＫＰ復号鍵生成部は、前記変数$\rho^{KP}(i)$が肯定形の組（t，$\vec{v}_i^{KP}$）である場合には、乱数θ_i^{KP}，$\eta_{i,i'}{}^{KP}$（$i=1,\ldots,L^{KP}$，$i'=1,\ldots,w_t^{KP}$）に基づき数３に示す要素$k^*_i{}^{KP}$を生成し、変数$\rho^{KP}(i)$が否定形の組$\neg(t,\vec{v}_i^{KP})$である場合には、乱数$\eta_{i,i'}{}^{KP}$（$i=1,\ldots,L^{KP}$，$i'=1,\ldots,w_t^{KP}$）に基づき数４に示す要素$k^*_i{}^{KP}$を生成し、

前記ＣＰ復号鍵生成部は、前記乱数δ^{CP}と乱数$\eta_{t,i}^{CP}$（$i=1$，

．．．，w_t^{CP}）に基づき数５に示す要素$k^*_t{}^{CP}$とを生成し、

前記暗号化装置では、

前記主暗号化データ生成部は、前記乱数ω^{KP}と乱数ζ，$\phi_{0,i}$（i＝1，．．．，z_0）とに基づき数６に示す要素c_0を生成し、

前記ＫＰ暗号化データ生成部は、前記乱数ω^{KP}と乱数$\phi_{t,i}^{KP}$（i＝1，．．．，z_t^{KP}）に基づき数７に示す要素c_t^{KP}とを生成し、

前記ＣＰ暗号化データ生成部は、前記変数ρ^{CP}（ｉ）が肯定形の組（ｔ，$v^{\rightarrow}{}_i^{CP}$）である場合には、乱数θ_i^{CP}，$\phi_{i,i'}^{CP}$（ｉ＝１，．．．，L^{CP}，ｉ’＝１，．．．，z_t^{CP}）に基づき数８に示す要素c_i^{CP}を生成し、変数ρ^{CP}（ｉ）が否定形の組￢（ｔ，$v^{\rightarrow}{}_i^{CP}$）である場合には、乱数$\phi_{i,i'}^{CP}$（ｉ＝１，．．．，L^{CP}，ｉ’＝１，．．．，z_t^{CP}）に基づき数９に示す要素c_i^{CP}を生成する

ことを特徴とする請求項１に記載の暗号処理システム。

[数2]

$$k_0^* := (-s_0^{KP}, \delta^{CP}, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*}$$

[数3]

$$k_i^{*KP} := (\overbrace{s_i^{KP} + \theta_i^{KP} v_{i,1}^{KP}, \theta_i^{KP} v_{i,2}^{KP}, \ldots, \theta_i^{KP} v_{i,n_t^{KP}}^{KP}}^{n_t^{KP}}, \overbrace{0^{u_t^{KP}}}^{u_t^{KP}}, \overbrace{\eta_{i,1}^{KP},\ldots,\eta_{i,w_t^{KP}}^{KP}}^{w_t^{KP}}, \overbrace{0^{z_t^{KP}}}^{z_t^{KP}})_{\mathbb{B}_t^{*KP}}$$

[数4]

$$k_i^{*KP} := (\overbrace{s_i^{KP} v_{i,1}^{KP}, \ldots, s_i^{KP} v_{i,n_t^{KP}}^{KP}}^{n_t^{KP}}, \overbrace{0^{u_t^{KP}}}^{u_t^{KP}}, \overbrace{\eta_{i,1}^{KP},\ldots,\eta_{i,w_t^{KP}}^{KP}}^{w_t^{KP}}, \overbrace{0^{z_t^{KP}}}^{z_t^{KP}})_{\mathbb{B}_t^{*KP}}$$

[数5]

$$k_t^{*\mathsf{CP}} := (\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{\eta_{t,1}^{\mathsf{CP}},\ldots,\eta_{t,w_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{w_t^{\mathsf{CP}}}, \overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{CP}}}$$

[数6]

$$c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\varphi_{0,1},\ldots,\varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0}$$

[数7]

$$c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}}\vec{x}_t^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}}, \overbrace{0^{w_t^{\mathsf{KP}}}}^{w_t^{\mathsf{KP}}}, \overbrace{\varphi_{t,1}^{\mathsf{KP}},\ldots,\varphi_{t,z_t^{\mathsf{KP}}}^{\mathsf{KP}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{\mathsf{KP}}}$$

[数8]

$$c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} v_{i,1}^{\mathsf{CP}}, \theta_i^{\mathsf{CP}} v_{i,2}^{\mathsf{CP}},\ldots,\theta_i^{\mathsf{CP}} v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\varphi_{i,1}^{\mathsf{CP}},\ldots,\varphi_{i,z_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}}$$

[数9]

$$c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} v_{i,1}^{\mathsf{CP}},\ldots,s_i^{\mathsf{CP}} v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\varphi_{i,1}^{\mathsf{CP}},\ldots,\varphi_{i,z_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}}$$

[請求項3] 前記暗号化装置は、さらに、

所定の値ｉについて$g_T = e(b_{0,i}, b^*_{0,i})$であり、ｔ＝１，．．．，$d^{KP}$の各整数ｔと所定の値ｉとについて$g_T = e(b_{t,i}, b^*_{t,i})$であり、ｔ＝１，．．．，$d^{CP}$の各整数ｔと所定の値ｉとについて$g_T = e(b_{t,i}, b^*_{t,i})$である値$g_T$を用いて、メッセ

ージｍを埋め込んだ要素$c_{d+1}=g_T^{\zeta}m$を生成するメッセージ暗号化データ生成部

を備え、

前記復号装置では、

前記データ取得部は、さらに前記要素c_{d+1}を含む暗号化データ$ct_{(\Gamma KP,\ SCP)}$を取得し、

前記復号装置は、さらに、

前記暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれる前記要素c_{d+1}を、前記ペアリング演算部が計算した値Ｋで除して、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１又は２に記載の暗号処理システム。

［請求項4］ 基底B_0及び基底B_0^*と、ｔ＝１，．．．，d^{KP}（d^{KP}は１以上の整数）の各整数ｔについての基底B_t^{KP}及び基底$B^*_t{}^{KP}$と、ｔ＝１，．．．，d^{CP}（d^{CP}は

１以上の整数）の各整数ｔについての基底B_t^{CP}及び基底$B^*_t{}^{CP}$とを用いて暗号処理を実行する暗号処理システムにおいて、復号鍵$sk_{(SKP,\ \Gamma CP)}$を生成する鍵生成装置であり、

ｉ＝１，．．．，L^{KP}（L^{KP}は１以上の整数）の各整数ｉについての変数$\rho^{KP}(i)$であって、識別情報ｔ（ｔ＝１，．．．，d^{KP}のいずれかの整数）と、属性ベクトル$\vec{v}_i^{KP}:=(v_{i,i'}{}^{KP})$（ｉ’＝１，．．．，$n_t^{KP}$，$n_t^{KP}$は１以上の整数）との肯定形の組（ｔ，$\vec{v}_i^{KP}$）又は否定形の組¬（ｔ，$\vec{v}_i^{KP}$）のいずれかである変数$\rho^{KP}(i)$と、$L^{KP}$行$r^{KP}$列（$r^{KP}$は１以上の整数）の所定の行列$M^{KP}$とを入力する第１ＫＰ情報入力部と、

ｔ＝１，．．．，d^{CP}の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}_t^{CP}:=(x_{t,i'}{}^{CP})$（ｉ’＝１，．．．，$n_t^{CP}$，$n_t^{CP}$は１以上の整数）とを有する属性集合$\Gamma^{CP}$を

入力する第１ＣＰ情報入力部と、

基底B^*_0の基底ベクトル$b^*_{0,p}$（ｐは所定の値）の係数として値$-s_0^{KP}$（$s_0^{KP}:=h^{\rightarrow KP}\cdot(f^{\rightarrow KP})^T$，$h^{\rightarrow KP}$及び$f^{\rightarrow KP}$は$r^{KP}$個の要素を有するベクトル）を設定し、基底ベクトル$b^*_{0,p'}$（ｐ’は前記ｐとは異なる所定の値）の係数として乱数δ^{CP}を設定し、基底ベクトル$b^*_{0,q}$（ｑは前記ｐ及び前記ｐ’とは異なる所定の値）の係数として所定の値κを設定して復号鍵$sk_{(SKP,\Gamma CP)}$の要素k^*_0を生成する主復号鍵生成部と、

前記$f^{\rightarrow KP}$と、前記第１ＫＰ情報入力部が入力した行列M^{KP}に基づき生成される列ベクトル$(s^{\rightarrow KP})^T:=(s_1^{KP},\ldots,s_i^{KP})^T:=M^{KP}\cdot(f^{\rightarrow KP})^T$（ｉ＝$L^{KP}$）と、乱数$\theta_i^{KP}$（ｉ＝１，．．．，$L^{KP}$）とに基づき、ｉ＝１，．．．，$L^{KP}$の各整数ｉについての要素$k^*_i{}^{KP}$を生成するＫＰ復号鍵生成部であって、ｉ＝１，．．．，L^{KP}の各整数ｉについて、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$v^{\rightarrow}_i{}^{KP}$）である場合には、その組の識別情報ｔが示す基底$B^*_t{}^{KP}$の基底ベクトル$b^*_{t,1}{}^{KP}$の係数として$s_i^{KP}+\theta_i^{KP}v_{i,1}^{KP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，n_t^{KP}の各整数ｉ’とが示す基底ベクトル$b^*_{t,i',KP}$の係数として$\theta_i^{KP}v_{i,i',KP}$を設定して復号鍵$sk_{(SKP,\Gamma CP)}$の要素$k^*_i{}^{KP}$を生成し、変数ρ^{KP}（ｉ）が否定形の組¬（ｔ，$v^{\rightarrow}_i{}^{KP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，n_t^{KP}の各整数ｉ’とが示す基底ベクトル$b^*_{t,i',KP}$の係数として$s_i^{KP}v_{i,i',KP}$を設定して復号鍵$sk_{(SKP,\Gamma CP)}$の要素$k^*_i{}^{KP}$を生成するＫＰ復号鍵生成部と、

前記第１ＣＰ情報入力部が入力した属性集合Γ^{CP}に含まれる各識別情報ｔについての要素$k^*_t{}^{CP}$を生成するＣＰ復号鍵生成部であって、基底$B^*_t{}^{CP}$の基底ベクトル$b^*_{t,i',CP}$（ｉ’＝１，．．．，n_t^{CP}）の係数として前記乱数δ^{CP}倍した$x_{t,i',CP}$を設定して復号鍵$sk_{(SKP,\Gamma CP)}$の要素$k^*_t{}^{CP}$を生成するＣＰ復号鍵生成部と

を備えることを特徴とする鍵生成装置。

[請求項5] 基底B_0及び基底B_0^*と、$t=1,\ldots,d^{KP}$（d^{KP}は１以上の整数）の各整数ｔについての基底B_t^{KP}及び基底$B^*_t{}^{KP}$と、$t=1,\ldots,d^{CP}$（d^{CP}は１以上の整数）の各整数ｔについての基底$B_t{}^{CP}$及び基底$B^*_t{}^{CP}$とを用いて暗号処理を実行する暗号処理システムにおいて、暗号化データ$ct_{(\Gamma^{KP},S^{CP})}$を生成する暗号化装置であり、

$t=1,\ldots,d^{KP}$の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}_t^{KP}:=(x_{t,i'}{}^{KP})$（$i'=1,\ldots,n_t{}^{KP}$）とを有する属性集合$\Gamma^{KP}$を入力する第２ＫＰ情報入力部と、

$i=1,\ldots,L^{CP}$（L^{CP}は１以上の整数）の各整数ｉについての変数$\rho^{CP}(i)$であって、識別情報ｔ（$t=1,\ldots,d^{CP}$のいずれかの整数）と、属性ベクトル$\vec{v}_i{}^{CP}:=(v_{i,i'}{}^{CP})$（$i'=1,\ldots,n_t{}^{CP}$）との肯定形の組$(t,\vec{v}_i{}^{CP})$又は否定形の組$\neg(t,\vec{v}_i{}^{CP})$のいずれかである変数$\rho^{CP}(i)$と、$L^{CP}$行$r^{CP}$列（$r^{CP}$は１以上の整数）の所定の行列$M^{CP}$とを入力する第２ＣＰ情報入力部と、

基底B_0の基底ベクトル$b_{0,p}$の係数として乱数ω^{KP}を設定し、基底ベクトル$b_{0,p'}$の係数として値$-s_0{}^{CP}$（$s_0{}^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$，$\vec{h}^{CP}$及び$\vec{f}^{CP}$は$r^{CP}$個の要素を有するベクトル）を設定し、基底ベクトル$b_{0,q}$の係数として乱数$\zeta$を設定して暗号化データ$ct_{(\Gamma^{KP},S^{CP})}$の要素$c_0$を生成する主暗号化データ生成部と、

前記第２ＫＰ情報入力部が入力した属性集合Γ^{KP}に含まれる各識別情報ｔについての要素$c_t{}^{KP}$を生成するＫＰ暗号化データ生成部であって、基底$B_t{}^{KP}$の基底ベクトル$b_{t,i'}{}^{KP}$（$i'=1,\ldots,n_t$）の係数として前記乱数ω^{KP}倍した$x_{t,i'}{}^{KP}$を設定して暗号化データ$ct_{(\Gamma^{KP},S^{CP})}$の要素$c_t{}^{KP}$を生成するＫＰ暗号化データ生成

部と、

前記$f^{\rightarrow CP}$と、前記第２ＣＰ情報入力部が入力した行列M^{CP}とに基づき生成される列ベクトル$(s^{\rightarrow CP})^{T}:=(s_1{}^{CP},\ldots,s_i{}^{CP})^{T}:=M^{CP}\cdot(f^{\rightarrow CP})^{T}$（$i=L^{CP}$）と、乱数$\theta_i{}^{CP}$（$i=1,\ldots,L^{CP}$）とに基づき、$i=1,\ldots,L^{CP}$の各整数ｉについての要素$c_i{}^{CP}$を生成するＣＰ暗号化データ生成部であって、$i=1,\ldots,L^{CP}$の各整数ｉについて、変数$\rho^{CP}(i)$が肯定形の組$(t, v^{\rightarrow}{}_i{}^{CP})$である場合には、その組の識別情報ｔが示す基底$B_t{}^{CP}$の基底ベクトル$b_{t,1}{}^{CP}$の係数として$s_i{}^{CP}+\theta_i{}^{CP}v_{i,1}{}^{CP}$を設定するとともに、前記識別情報ｔと$i'=2,\ldots,n_t{}^{CP}$の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$\theta_i{}^{CP}v_{i,i',CP}$を設定して暗号化データ$ct_{(\Gamma KP,SCP)}$の要素$c_i{}^{CP}$を生成し、変数$\rho^{CP}(i)$が否定形の組$\neg(t, v^{\rightarrow}{}_i{}^{CP})$である場合には、その組の識別情報ｔと$i'=1,\ldots,n_t{}^{CP}$の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$s_i{}^{CP}v_{i,i',CP}$を設定して暗号化データ$ct_{(\Gamma KP,SCP)}$の要素$c_i{}^{CP}$を生成するＣＰ暗号化データ生成部と

を備えることを特徴とする暗号化装置。

［請求項6］ 基底B_0及び基底$B_0{}^{*}$と、$t=1,\ldots,d^{KP}$（d^{KP}は１以上の整数）の各整数ｔについての基底$B_t{}^{KP}$及び基底$B^{*}{}_t{}^{KP}$と、$t=1,\ldots,d^{CP}$（d^{CP}は１以上の整数）の各整数ｔについての基底$B_t{}^{CP}$及び基底$B^{*}{}_t{}^{CP}$とを用いて暗号処理を実行する暗号処理システムにおいて、暗号化データ$ct_{(\Gamma KP,SCP)}$を復号鍵$sk_{(SKP,\Gamma CP)}$で復号する復号装置であり、

$t=1,\ldots,d^{KP}$の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$x^{\rightarrow}{}_t{}^{KP}:=(x_{t,i',KP})$（$i'=1,\ldots,n_t{}^{KP}$，$n_t{}^{KP}$は１以上の整数）とを有する属性集合$\Gamma^{KP}$と、

ｉ＝１，．．．，L^{CP}（L^{CP}は１以上の整数）の各整数ｉについての変数ρ^{CP}（ｉ）であって、識別情報ｔ（ｔ＝１，．．．，d^{CP}のいずれかの整数）と、属性ベクトル$\vec{v}_i^{CP}$：＝（$v_{i,i'}^{CP}$）（ｉ’＝１，．．．，n_t^{CP}，n_t^{CP}は１以上の整数）との肯定形の組（ｔ，$\vec{v}_i^{CP}$）又は否定形の組￢（ｔ，$\vec{v}_i^{CP}$）のいずれかである変数ρ^{CP}（ｉ）と、

L^{CP}行r^{CP}列（r^{CP}は１以上の整数）の所定の行列M^{CP}と、

基底B_0の基底ベクトル$b_{0,p}$の係数として乱数ω^{KP}が設定され、基底ベクトル$b_{0,p'}$の係数として値$-s_0^{CP}$（s_0^{CP}：＝$\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$，$\vec{h}^{CP}$及び$\vec{f}^{CP}$は$r^{CP}$個の要素を有するベクトル）が設定され、基底ベクトル$b_{0,q}$の係数として乱数ζが設定された要素c_0と、

前記属性集合Γ^{KP}に含まれる各識別情報ｔについて、基底B_t^{KP}の基底ベクトル$b_{t,i',KP}$（ｉ’＝１，．．．，n_t）の係数として前記乱数ω^{KP}倍した$x_{t,i',KP}$が設定された要素c_t^{KP}と、

前記$\vec{f}^{CP}$と、前記行列M^{CP}とに基づき生成される列ベクトル（$\vec{s}^{CP}$）^{T}：＝（s_1^{CP}，．．．，s_i^{CP}）^{T}：＝$M^{CP}\cdot(\vec{f}^{CP})^T$（ｉ＝$L^{CP}$）と、乱数

θ_i^{CP}（ｉ＝１，．．．，L^{CP}）とに基づき、ｉ＝１，．．．，L^{CP}の各整数ｉについて生成された要素c_i^{CP}であって、ｉ＝１，．．．，L^{CP}の各整数ｉについて、変数ρ^{CP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{CP}$）である場合には、その組の識別情報ｔが示す基底B_t^{CP}の基底ベクトル$b_{t,1}^{CP}$の係数として$s_i^{CP}+\theta_i^{CP}v_{i,1}^{CP}$が設定されるとともに、前記識別情報ｔとｉ’＝２，．．．，n_t^{CP}の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$\theta_i^{CP}v_{i,i',CP}$が設定され、変数ρ^{CP}（ｉ）が否定形の組￢（ｔ，$\vec{v}_i^{CP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，n_t^{CP}の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$s_i^{CP}v_{i,i',CP}$が設定さ

れた要素c_i^{CP}と

を含む暗号化データ$ct_{(\Gamma^{KP}, SCP)}$を取得するデータ取得部と、

$i=1,\ldots,L^{KP}$（L^{KP}は１以上の整数）の各整数iについての変数$\rho^{KP}(i)$であって、識別情報t（$t=1,\ldots,d^{KP}$のいずれかの整数）と、属性ベクトル$\vec{v}_i^{KP}:=(v_{i,i'}^{KP})$（$i'=1,\ldots,n_t^{KP}$）との肯定形の組$(t, \vec{v}_i^{KP})$又は否定形の組$\neg(t, \vec{v}_i^{KP})$のいずれかである変数$\rho^{KP}(i)$と、

L^{KP}行r^{KP}列（r^{KP}は１以上の整数）の所定の行列M^{KP}と、

$t=1,\ldots,d^{CP}$の少なくとも１つ以上の整数tについて、識別情報tと、属性ベクトル$\vec{x}_t^{CP}:=(x_{t,i'}^{CP})$（$i'=1,\ldots,n_t^{CP}$）とを有する属性集合$\Gamma^{CP}$と

基底B^*_0の基底ベクトル$b^*_{0,p}$（pは所定の値）の係数として値$-s_0^{KP}$（$s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$，$\vec{h}^{KP}$及び$\vec{f}^{KP}$は$r^{KP}$個の要素を有するベクトル）が設定され、基底ベクトル$b^*_{0,p'}$（p'は前記pとは異なる所定の値）の係数として乱数δ^{CP}が設定され、基底ベクトル$b^*_{0,q}$（qは前記p及び前記p'とは異なる所定の値）の係数として所定の値κが設定された要素k^*_0と、

前記$\vec{f}^{KP}$と、前記第１ＫＰ情報入力部が入力した行列M^{KP}に基づき生成される列ベクトル$(\vec{s}^{KP})^T:=(s_1^{KP},\ldots,s_i^{KP})^T:=M^{KP}\cdot(\vec{f}^{KP})^T$（$i=L^{KP}$）と、乱数$\theta_i^{KP}$（$i=1,\ldots,L^{KP}$）とに基づき、$i=1,\ldots,L^{KP}$の各整数$i$について生成された要素$k^*_i{}^{KP}$であって、$i=1,\ldots,L^{KP}$の各整数$i$について、変数$\rho^{KP}(i)$が肯定形の組$(t, \vec{v}_i^{KP})$である場合には、その組の識別情報$t$が示す基底$B^*_t{}^{KP}$の基底ベクトル$b^*_{t,1}{}^{KP}$の係数として$s_i^{KP}+\theta_i^{KP}v_{i,1}^{KP}$が設定されるとともに、前記識別情報$t$と$i'=2,\ldots,n_t^{KP}$の各整数$i'$とが示す基底ベクトル$b^*_{t,i',KP}$の係数として$\theta_i^{KP}v_{i,i',KP}$が設定され、変数$\rho^{KP}(i)$が否定形の組$\neg(t, \vec{v}_i^{KP})$である場合には、その組の識

別情報ｔとｉ’＝１，．．．，n_t^{KP}の各整数ｉ’とが示す基底ベクトル$b^*_{t,i',KP}$の係数として$s_i^{KP} v_{i,i',KP}$が設定された要素$k^*_i{}^{KP}$と、

前記属性集合Γ^{CP}に含まれる各識別情報ｔについて、基底$B^*_t{}^{CP}$の基底ベクトル$b^*_{t,i',CP}$（ｉ’＝１，．．．，n_t^{CP}）の係数として前記乱数δ^{CP}倍した$x_{t,i',CP}$が設定された要素$k^*_t{}^{CP}$と

を含む復号鍵$sk_{(SKP,\Gamma CP)}$を取得する復号鍵取得部と、

前記データ取得部が取得した暗号化データ$ct_{(\Gamma KP,SCP)}$に含まれる属性集合Γ^{KP}と、前記復号鍵取得部が取得した復号鍵$sk_{(SKP,\Gamma CP)}$に含まれる変数ρ^{KP}（ｉ）とに基づき、ｉ＝１，．．．，L^{KP}の各整数ｉのうち、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{KP}$）であり、かつ、その組の$\vec{v}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$\vec{x}_t^{KP}$との内積が０となるｉと、変数ρ^{KP}（ｉ）が否定形の組￢（ｔ，$\vec{v}_i^{KP}$）であり、かつ、その組の$\vec{v}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$\vec{x}_t^{KP}$との内積が０とならないｉとの集合I^{KP}を特定するとともに、特定した集合I^{KP}に含まれるｉについて、$\alpha_i^{KP} M_i^{KP}$を合計した場合に前記$h\rightarrow^{KP}$となる補完係数α_i^{KP}を計算するＫＰ補完係数計算部と、

前記暗号化データ$ct_{(\Gamma KP,SCP)}$に含まれるｉ＝１，．．．，L^{CP}の各整数

ｉについての変数ρ^{CP}（ｉ）と、前記復号鍵$sk_{(SKP,\Gamma CP)}$に含まれる属性集合Γ^{CP}とに基づき、ｉ＝１，．．．，L^{CP}の各整数ｉのうち、変数ρ^{CP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{CP}$）であり、かつ、その組の$\vec{v}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$\vec{x}_t^{CP}$との内積が０となるｉと、変数ρ^{CP}（ｉ）が否定形の組￢（ｔ，$\vec{v}_i^{CP}$）であり、かつ、その組の$\vec{v}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$\vec{x}_t^{CP}$との内積が０とならないｉとの集合I^{CP}を特定するとともに、特定した集合I^{CP}に含まれるｉについて、α_i

$^{CP}M_i{}^{CP}$を合計した場合に前記ｈ→^{CP}となる補完係数$\alpha_i{}^{CP}$を計算するＣＰ補完係数計算部と、

前記暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$に含まれる要素ｃ$_0$と要素ｃ$_t{}^{KP}$と要素ｃ$_i{}^{CP}$と、前記復号鍵ｓｋ$_{(SKP,\ \Gamma CP)}$に含まれる要素ｋ＊$_0$と要素ｋ＊$_i{}^{KP}$と要素ｋ＊$_t{}^{CP}$とについて、前記ＫＰ補完係数計算部が特定した集合Ｉ^{KP}と、前記ＫＰ補完係数計算部が計算した補完係数$\alpha_i{}^{KP}$と、前記ＣＰ補完係数計算部が特定した集合Ｉ^{CP}と、前記ＣＰ補完係数計算部が計算した補完係数$\alpha_i{}^{CP}$とに基づき、数１０に示すペアリング演算を行い値Ｋを計算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。

[数10]

$$K := e(c_0, k_0^*)\cdot \prod_{i\in I^{KP}\wedge\rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i\in I^{KP}\wedge\rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP}\cdot\vec{x}_t^{KP})} \cdot \prod_{i\in I^{CP}\wedge\rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i\in I^{CP}\wedge\rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP}\cdot\vec{x}_t^{CP})}$$

[請求項7] 基底Ｂ$_0$及び基底Ｂ$_0$＊と、ｔ＝１，．．．，ｄ^{KP}（ｄ^{KP}は１以上の整数）の各整数ｔについての基底Ｂ$_t{}^{KP}$及び基底Ｂ＊$_t{}^{KP}$と、ｔ＝１，．．．，ｄ^{CP}（ｄ^{CP}は１以上の整数）の各整数ｔについての基底Ｂ$_t{}^{CP}$及び基底Ｂ＊$_t{}^{CP}$とを用いた暗号処理方法であり、

鍵生成装置が、ｉ＝１，．．．，Ｌ^{KP}（Ｌ^{KP}は１以上の整数）の各整数ｉについての変数ρ^{KP}（ｉ）であって、識別情報ｔ（ｔ＝１，．．．，ｄ^{KP}のいずれかの整数）と、属性ベクトルｖ$\rightarrow_i{}^{KP}$：＝（ｖ$_{i,\ i',}{}^{KP}$）（ｉ’＝１，．．．，ｎ$_t{}^{KP}$，ｎ$_t{}^{KP}$は１以上の整数）との肯定形の組（ｔ，ｖ$\rightarrow_i{}^{KP}$）又は否定形の組￢（ｔ，ｖ$\rightarrow_i{}^{KP}$）のい

ずれかである変数ρ^{KP}（ｉ）と、L^{KP}行r^{KP}列（r^{KP}は１以上の整数）の所定の行列M^{KP}とを入力する第１ＫＰ情報入力工程と、

前記鍵生成装置が、ｔ＝１，．．．，d^{CP}の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}_t^{CP}:=(x_{t,i',CP})$（ｉ’＝１，．．．，$n_t^{CP}$，$n_t^{CP}$は１以上の整数）とを有する属性集合$\Gamma^{CP}$を入力する第１ＣＰ情報入力工程と、

前記鍵生成装置が、基底B^*_0の基底ベクトル$b^*_{0,p}$（ｐは所定の値）の係数として値$-s_0^{KP}$（$s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$，$\vec{h}^{KP}$及び$\vec{f}^{KP}$は$r^{KP}$個の要素を有するベクトル）を設定し、基底ベクトル$b^*_{0,p'}$（ｐ’は前記ｐとは
異なる所定の値）の係数として乱数δ^{CP}を設定し、基底ベクトル$b^*_{0,q}$（ｑは前記ｐ及び前記ｐ’とは異なる所定の値）の係数として所定の値κを設定して要素k^*_0を生成する主復号鍵生成工程と、

前記鍵生成装置が、前記$\vec{f}^{KP}$と、前記第１ＫＰ情報入力工程で入力した行列M^{KP}に基づき生成される列ベクトル$(\vec{s}^{KP})^T:=(s_1^{KP},．．．,s_i^{KP})^T:=M^{KP}\cdot(\vec{f}^{KP})^T$（ｉ＝$L^{KP}$）と、乱数$\theta_i^{KP}$（ｉ＝１，．．．，$L^{KP}$）とに基づき、ｉ＝１，．．．，$L^{KP}$の各整数ｉについての要素$k^*_i{}^{KP}$を生成するＫＰ復号鍵生成工程であって、ｉ＝１，．．．，L^{KP}の各整数ｉについて、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{KP}$）である場合には、その組の識別情報ｔが示す基底$B^*_t{}^{KP}$の基底ベクトル$b^*_{t,1}{}^{KP}$の係数として$s_i^{KP}+\theta_i^{KP}v_{i,1}^{KP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，n_t^{KP}の各整数ｉ’とが示す基底ベクトル$b^*_{t,i',KP}$の係数として$\theta_i^{KP}v_{i,i',KP}$を設定して要素$k^*_i{}^{KP}$を生成し、変数ρ^{KP}（ｉ）が否定形の組¬（ｔ，$\vec{v}_i^{KP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，n_t^{KP}の各整数ｉ’とが示す基底ベクトル$b^*_{t,i',KP}$の係数として$s_i^{KP}v_{i,i',KP}$を設定して要素$k^*_i{}^{KP}$を生成するＫＰ復号鍵生成工程と、

前記鍵生成装置が、前記第１ＣＰ情報入力工程で入力した属性集合Γ^{CP}に含まれる各識別情報ｔについての要素ｋ$^{*}{}_{t}{}^{CP}$を生成するＣＰ復号鍵生成工程であって、基底Ｂ$^{*}{}_{t}{}^{CP}$の基底ベクトルｂ$^{*}{}_{t,i'}{}^{CP}$（ｉ’＝１，．．．，ｎ$_{t}{}^{CP}$）の係数として前記乱数δ^{CP}倍したｘ$_{t,i'}{}^{CP}$を設定して要素ｋ$^{*}{}_{t}{}^{CP}$を生成するＣＰ復号鍵生成工程と、

暗号化装置が、ｔ＝１，．．．，ｄ^{KP}の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}{}_{t}{}^{KP}$：＝（ｘ$_{t,i'}{}^{KP}$）（ｉ’＝１，．．．，ｎ$_{t}{}^{KP}$）とを有する属性集合Γ^{KP}を入力する第２ＫＰ情報入力工程と、

前記暗号化装置が、ｉ＝１，．．．，Ｌ^{CP}（Ｌ^{CP}は１以上の整数）の各整数ｉについての変数ρ^{CP}（ｉ）であって、識別情報ｔ（ｔ＝１，．．．，ｄ^{CP}のいずれかの整数）と、属性ベクトル$\vec{v}{}_{i}{}^{CP}$：＝（ｖ$_{i,i'}{}^{CP}$）（ｉ’＝１，．．．，ｎ$_{t}{}^{CP}$）との肯定形の組（ｔ，$\vec{v}{}_{i}{}^{CP}$）又は否定形の組¬（ｔ，$\vec{v}{}_{i}{}^{CP}$）のいずれかである変数ρ^{CP}（ｉ）と、Ｌ^{CP}行ｒ^{CP}列（ｒ^{CP}は１以上の整数）の所定の行列Ｍ^{CP}とを入力する第２ＣＰ情報入力工程と、

前記暗号化装置が、基底Ｂ$_{0}$の基底ベクトルｂ$_{0,p}$の係数として乱数ω^{KP}を設定し、基底ベクトルｂ$_{0,p'}$の係数として値－ｓ$_{0}{}^{CP}$（ｓ$_{0}{}^{CP}$：＝$\vec{h}{}^{CP}$・（$\vec{f}{}^{CP}$）^{T}，$\vec{h}{}^{CP}$及び$\vec{f}{}^{CP}$はｒ^{CP}個の要素を有するベクトル）を設定し、基底ベクトルｂ$_{0,q}$の係数として乱数ζを設定して要素ｃ$_{0}$を生成する主暗号化データ生成工程と、

前記暗号化装置が、前記第２ＫＰ情報入力工程で入力した属性集合Γ^{KP}に含まれる各識別情報ｔについての要素ｃ$_{t}{}^{KP}$を生成するＫＰ暗号化データ生成工程であって、基底Ｂ$_{t}{}^{KP}$の基底ベクトルｂ$_{t,i'}{}^{KP}$（ｉ’＝１，．．．，ｎ$_{t}$）の係数として前記乱数ω^{KP}倍したｘ$_{t,i'}{}^{KP}$を設定して要素ｃ$_{t}{}^{KP}$を生成するＫＰ暗号化データ生成工程と、

前記暗号化装置が、前記$\vec{f}{}^{CP}$と、前記第２ＣＰ情報入力工程で入力した行列Ｍ^{CP}とに基づき生成される列ベクトル（$\vec{s}{}^{CP}$）^{T}：＝（

$s_1^{CP}, \ldots, s_i^{CP})^T := M^{CP} \cdot (f^{\rightarrow CP})^T$（$i = L^{CP}$）と、乱数$\theta_i^{CP}$（$i = 1, \ldots, L^{CP}$）とに基づき、$i = 1, \ldots, L^{CP}$の各整数$i$についての要素$c_i^{CP}$を生成するＣＰ暗号化データ生成工程であって、$i = 1, \ldots, L^{CP}$の各整数$i$について、変数$\rho^{CP}(i)$が肯定形の組（$t$，$v^{\rightarrow}{}_i^{CP}$）である場合には、その組の識別情報$t$が示す基底$B_t^{CP}$の基底ベクトル$b_{t,1}^{CP}$の係数として$s_i^{CP} + \theta_i^{CP} v_{i,1}^{CP}$を設定するとともに、前記識別情報$t$と$i' = 2, \ldots, n_t^{CP}$の各整数$i'$とが示す基底ベクトル$b_{t,i',CP}$の係数として$\theta_i^{CP} v_{i,i',CP}$を設定して要素$c_i^{CP}$を生成し、変数$\rho^{CP}(i)$が否定形の組¬（$t$，$v^{\rightarrow}{}_i^{CP}$）である場合には、その組の識別情報$t$と$i' = 1, \ldots, n_t^{CP}$の各整数$i'$とが示す基底ベクトル$b_{t,i',CP}$の係数として$s_i^{CP} v_{i,i',CP}$を設定して要素$c_i^{CP}$を生成するＣＰ暗号化データ生成工程と、

復号装置が、前記主暗号化データ生成工程で生成した要素c_0と、前記ＫＰ暗号化データ生成工程で生成した要素c_t^{KP}と、前記ＣＰ暗号化データ生成工程で生成した要素c_i^{CP}と、前記属性集合Γ^{KP}と、前記変数$\rho^{CP}(i)$とを含む暗号化データ$ct_{(\Gamma KP, SCP)}$を取得するデータ取得工程と、

前記復号装置が、前記主復号鍵生成工程で生成した要素k^*_0と、前記ＫＰ復号鍵生成工程で生成した要素$k^*_i{}^{KP}$と、前記ＣＰ復号鍵生成工程で生成した要素$k^*_t{}^{CP}$と、前記変数$\rho^{KP}(i)$と、前記属性集合Γ^{CP}とを含む復号鍵$sk_{(SKP, \Gamma CP)}$を取得する復号鍵取得工程と、

前記復号装置が、前記データ取得工程で取得した暗号化データ$ct_{(\Gamma KP, SCP)}$に含まれる属性集合Γ^{KP}と、前記復号鍵取得工程で取得した復号鍵$sk_{(SKP, \Gamma CP)}$に含まれる変数$\rho^{KP}(i)$とに基づき、$i = 1, \ldots, L^{KP}$の各整数iのうち、変数$\rho^{KP}(i)$が肯定形の組（t，$v^{\rightarrow}{}_i^{KP}$）であり、かつ、その組の$v^{\rightarrow}{}_i^{KP}$と、その組の識

別情報ｔが示すΓ^{KP}に含まれる$x\vec{}_t^{KP}$との内積が０となるｉと、変数ρ_i^{KP}（ｉ）が否定形の組￢（ｔ，$v\vec{}_i^{KP}$）であり、かつ、その組の$v\vec{}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$x\vec{}_t^{KP}$との内積が０とならないｉとの集合Ｉ^{KP}を特定するとともに、特定した集合Ｉ^{KP}に含まれるｉについて、$\alpha_i^{KP}M_i^{KP}$を合計した場合に前記$h\vec{}^{KP}$となる補完係数α_i^{KP}を計算するＫＰ補完係数計算工程と、

前記復号装置が、前記暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれるｉ＝１，．．．，Ｌ^{CP}の各整数ｉについての変数ρ_i^{CP}（ｉ）と、前記復号鍵$sk_{(SKP,\ \Gamma CP)}$に含まれる属性集合Γ^{CP}とに基づき、ｉ＝１，．．．，Ｌ^{CP}の各整数ｉのうち、変数ρ_i^{CP}（ｉ）が肯定形の組（ｔ，$v\vec{}_i^{CP}$）であり、かつ、その組の$v\vec{}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$x\vec{}_t^{CP}$との内積が０となるｉと、変数ρ_i^{CP}（ｉ）が否定形の組￢（ｔ，$v\vec{}_i^{CP}$）であり、かつ、その組の$v\vec{}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$x\vec{}_t^{CP}$との内積が０とならないｉとの集合Ｉ^{CP}を特定するとともに、特定した集合Ｉ^{CP}に含まれるｉについて、$\alpha_i^{CP}M_i^{CP}$を合計した場合に前記$h\vec{}^{CP}$となる補完係数α_i^{CP}を計算するＣＰ補完係数計算工程と、

前記復号装置が、前記暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれる要素c_0と要素c_t^{KP}と要素c_i^{CP}と、前記復号鍵$sk_{(SKP,\ \Gamma CP)}$に含まれる要素k^*_0と要素$k^*_i{}^{KP}$と要素$k^*_t{}^{CP}$とについて、前記ＫＰ補完係数計算工程で特定した集合Ｉ^{KP}と、前記ＫＰ補完係数計算工程で計算した補完係数α_i^{KP}と、前記ＣＰ補完係数計算工程で特定した集合Ｉ^{CP}と、前記ＣＰ補完係数計算工程で計算した補完係数α_i^{CP}とに基づき、数１に示すペアリング演算を行い値Ｋを計算するペアリング演算工程と

を備えることを特徴とする暗号処理方法。

[数11]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

[請求項8] 鍵生成プログラムと暗号化プログラムと復号プログラムとを備え、基底B_0及び基底B_0^*と、$t=1,\ldots,d^{KP}$（d^{KP}は１以上の整数）の各整数ｔについての基底B_t^{KP}及び基底$B^*_t{}^{KP}$と、$t=1,\ldots,d^{CP}$（d^{CP}は１以上の整数）の各整数ｔについての基底B_t^{CP}及び基底$B^*_t{}^{CP}$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、

前記鍵生成プログラムは、

$i=1,\ldots,L^{KP}$（L^{KP}は１以上の整数）の各整数ｉについての変数$\rho^{KP}(i)$であって、識別情報ｔ（$t=1,\ldots,d^{KP}$のいずれかの整数）と、属性ベクトル$\vec{v}_i^{KP} := (v_{i,i'}{}^{KP})$（$i'=1,\ldots,n_t^{KP}$，$n_t^{KP}$は１以上の整数）との肯定形の組（ｔ，$\vec{v}_i^{KP}$）又は否定形の組¬（ｔ，$\vec{v}_i^{KP}$）のいずれかである変数$\rho^{KP}(i)$と、$L^{KP}$行$r^{KP}$列（$r^{KP}$は１以上の整数）の所定の行列$M^{KP}$とを入力する第１ＫＰ情報入力処理と、

$t=1,\ldots,d^{CP}$の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}_t^{CP} := (x_{t,i'}{}^{CP})$（$i'=1,\ldots,n_t^{CP}$，$n_t^{CP}$は１以上の整数）とを有する属性集合$\Gamma^{CP}$を入力する第１ＣＰ情報入力処理と、

基底B^*_0の基底ベクトル$b^*_{0,p}$（ｐは所定の値）の係数として値

－s_0^{KP}（s_0^{KP}：＝$h^{\rightarrow KP}$・（$f^{\rightarrow KP}$）^{T}，$h^{\rightarrow KP}$及び$f^{\rightarrow KP}$はr^{KP}個の要素を有するベクトル）を設定し、基底ベクトル$b^*_{0,p'}$（p'は前記pとは異なる所定の値）の係数として乱数δ^{CP}を設定し、基底ベクトル$b^*_{0,q}$（qは前記p及び前記p'とは異なる所定の値）の係数として所定の値κを設定して要素k^*_0を生成する主復号鍵生成処理と、

前記$f^{\rightarrow KP}$と、前記第１ＫＰ情報入力処理で入力した行列M^{KP}に基づき生成される列ベクトル（$s^{\rightarrow KP}$）^{T}：＝（s_1^{KP}，．．．，s_i^{KP}）^{T}：＝M^{KP}・（$f^{\rightarrow KP}$）^{T}（ｉ＝L^{KP}）と、乱数θ_i^{KP}（ｉ＝１，．．，L^{KP}）とに基づき、ｉ＝１，．．．，L^{KP}の各整数ｉについての要素$k^*_i^{KP}$を生成するＫＰ復号鍵生成処理であって、ｉ＝１，．．．，L^{KP}の各整数ｉについて、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$v^{\rightarrow}_i^{KP}$）である場合には、その組の識別情報ｔが示す基底$B^*_t^{KP}$の基底ベクトル$b^*_{t,1}^{KP}$の係数として$s_i^{KP}+\theta_i^{KP}v_{i,1}^{KP}$を設定するとともに、前記識別情報ｔとｉ'＝２，．．．，n_t^{KP}の各整数ｉ'とが示す基底ベクトル$b^*_{t,i'}^{KP}$の係数として$\theta_i^{KP}v_{i,i'}^{KP}$を設定して要素$k^*_i^{KP}$を生成し、変数$\rho^{KP}$（ｉ）が否定形の組￢（ｔ，$v^{\rightarrow}_i^{KP}$）である場合には、その組の識別情報ｔとｉ'＝１，．．．，n_t^{KP}の各整数ｉ'とが示す基底ベクトル$b^*_{t,i'}^{KP}$の係数として$s_i^{KP}v_{i,i'}^{KP}$を設定して要素$k^*_i^{KP}$を生成するＫＰ復号鍵生成処理と、

前記第１ＣＰ情報入力処理で入力した属性集合Γ^{CP}に含まれる各識別情報ｔについての要素$k^*_t^{CP}$を生成するＣＰ復号鍵生成処理であって、基底$B^*_t^{CP}$の基底ベクトル$b^*_{t,i'}^{CP}$（ｉ'＝１，．．．，n_t^{CP}）の係数として前記乱数δ^{CP}倍した$x_{t,i'}^{CP}$を設定して要素$k^*_t^{CP}$を生成するＣＰ復号鍵生成処理と

をコンピュータに実行させ、

前記暗号化プログラムは、

ｔ＝１，．．．．，ｄ^{KP}の少なくとも１つ以上の整数ｔについて、識別情報ｔと、属性ベクトル$\vec{x}_t^{KP}$：＝（$x_{t,i'}^{KP}$）（ｉ’＝１，．．．．，n_t^{KP}）とを有する属性集合Γ^{KP}を入力する第２ＫＰ情報入力処理と、

ｉ＝１，．．．．，Ｌ^{CP}（Ｌ^{CP}は１以上の整数）の各整数ｉについての変数ρ^{CP}（ｉ）であって、識別情報ｔ（ｔ＝１，．．．．，ｄ^{CP}のいずれかの整数）と、属性ベクトル$\vec{v}_i^{CP}$：＝（$v_{i,i'}^{CP}$）（ｉ’＝１，．．．．，n_t^{CP}）との肯定形の組（ｔ，$\vec{v}_i^{CP}$）又は否定形の組¬（ｔ，$\vec{v}_i^{CP}$）のいずれかである変数ρ^{CP}（ｉ）と、Ｌ^{CP}行ｒ^{CP}列（ｒ^{CP}は１以上の整数）の所定の行列Ｍ^{CP}とを入力する第２ＣＰ情報入力処理と、

基底B_0の基底ベクトル$b_{0,p}$の係数として乱数ω^{KP}を設定し、基底ベクトル$b_{0,p'}$の係数として値－s_0^{CP}（s_0^{CP}：＝$\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$，$\vec{h}^{CP}$及び$\vec{f}^{CP}$はｒ^{CP}個の要素を有するベクトル）を設定し、基底ベクトル$b_{0,q}$の係数として乱数ζを設定して要素c_0を生成する主暗号化データ生成処理と、

前記第２ＫＰ情報入力処理で入力した属性集合Γ^{KP}に含まれる各識別情報ｔについての要素c_t^{KP}を生成するＫＰ暗号化データ生成処理であって、基底B_t^{KP}の基底ベクトル$b_{t,i'}^{KP}$（ｉ’＝１，．．．，n_t）の係数として前記乱数ω^{KP}倍した$x_{t,i'}^{KP}$を設定して要素c_t^{KP}を生成するＫＰ暗号化データ生成処理と、

前記$\vec{f}^{CP}$と、前記第２ＣＰ情報入力処理で入力した行列Ｍ^{CP}とに基づき生成される列ベクトル（$\vec{s}^{CP}$）^{T}：＝（s_1^{CP}，．．．，s_i^{CP}）^{T}：＝Ｍ$^{CP}\cdot(\vec{f}^{CP})^T$（ｉ＝Ｌ^{CP}）と、乱数$\theta_i^{CP}$（ｉ＝１，．．．．，Ｌ^{CP}）とに基づき、ｉ＝１，．．．．，Ｌ^{CP}の各整数ｉについての要素c_i^{CP}を生成するＣＰ暗号化データ生成処理であって、ｉ＝１，．．．．，Ｌ^{CP}の各整数ｉについて、変数ρ^{CP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{CP}$）である場合には、その組の識別情報ｔが示す

基底B_t^{CP}の基底ベクトル$b_{t,1}^{CP}$の係数として$s_i^{CP}+\theta_i^{CP}v_{i,1}^{CP}$を設定するとともに、前記識別情報ｔとｉ’＝２，．．．，n_t^{CP}の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$\theta_i^{CP}v_{i,i',CP}$を設定して要素c_i^{CP}を生成し、変数ρ^{CP}（ｉ）が否定形の組¬（ｔ，$\vec{v}_i^{CP}$）である場合には、その組の識別情報ｔとｉ’＝１，．．．，n_t^{CP}の各整数ｉ’とが示す基底ベクトル$b_{t,i',CP}$の係数として$s_i^{CP}v_{i,i',CP}$を設定して要素c_i^{CP}を生成するＣＰ暗号化データ生成処理と

をコンピュータに実行させ、

前記復号プログラムは、

前記主暗号化データ生成処理で生成した要素c_0と、前記ＫＰ暗号化データ生成処理で生成した要素c_t^{KP}と、前記ＣＰ暗号化データ生成処理で生成した要素c_i^{CP}と、前記属性集合Γ^{KP}と、前記変数ρ^{CP}（ｉ）とを含む暗号化データ$ct_{(\Gamma KP,\ SCP)}$を取得するデータ取得処理と、

前記主復号鍵生成処理で生成した要素k^*_0と、前記ＫＰ復号鍵生成処理で生成した要素$k^*_i{}^{KP}$と、前記ＣＰ復号鍵生成処理で生成した要素$k^*_t{}^{CP}$と、前記変数ρ^{KP}（ｉ）と、前記属性集合Γ^{CP}とを含む復号鍵$sk_{(SKP,\ \Gamma CP)}$を取得する復号鍵取得処理と、

前記データ取得処理で取得した暗号化データ$ct_{(\Gamma KP,\ SCP)}$に含まれる属性集合Γ^{KP}と、前記復号鍵取得処理で取得した復号鍵$sk_{(SKP,\ \Gamma CP)}$に含まれる変数ρ^{KP}（ｉ）とに基づき、ｉ＝１，．．．，L^{KP}の各整数ｉのうち、変数ρ^{KP}（ｉ）が肯定形の組（ｔ，$\vec{v}_i^{KP}$）であり、かつ、その組の$\vec{v}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$\vec{x}_t^{KP}$との内積が０となるｉと、変数ρ^{KP}（ｉ）が否定形の組¬（ｔ，$\vec{v}_i^{KP}$）であり、かつ、その組の$\vec{v}_i^{KP}$と、その組の識別情報ｔが示すΓ^{KP}に含まれる$\vec{x}_t^{KP}$との内積が０とならないｉとの集合I^{KP}を特定するとともに、特定した集合I^{KP}に含まれる

ｉについて、$\alpha_i^{KP}M_i^{KP}$を合計した場合に前記ｈ$\rightarrow^{KP}$となる補完係数α_i^{KP}を計算するＫＰ補完係数計算処理と、

前記暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$に含まれるｉ＝１，．．．，L^{CP}の各整数ｉについての変数ρ^{CP}（ｉ）と、前記復号鍵ｓｋ$_{(SKP,\ \Gamma CP)}$に含まれる属性集合Γ^{CP}とに基づき、ｉ＝１，．．．，L^{CP}の各整数ｉのうち、変数ρ^{CP}（ｉ）が肯定形の組（ｔ，$v\vec{}_i^{CP}$）であり、かつ、その組の$v\vec{}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$x\vec{}_t^{CP}$との内積が０となるｉと、変数ρ^{CP}（ｉ）が否定形の組￢（ｔ，$v\vec{}_i^{CP}$）であり、かつ、その組の$v\vec{}_i^{CP}$と、その組の識別情報ｔが示すΓ^{CP}に含まれる$x\vec{}_t^{CP}$との内積が０とならないｉとの集合I^{CP}を特定するとともに、特定した集合I^{CP}に含まれるｉについて、$\alpha_i^{CP}M_i^{CP}$を合計した場合に前記ｈ$\rightarrow^{CP}$となる補完係数α_i^{CP}を計算するＣＰ補完係数計算処理と、

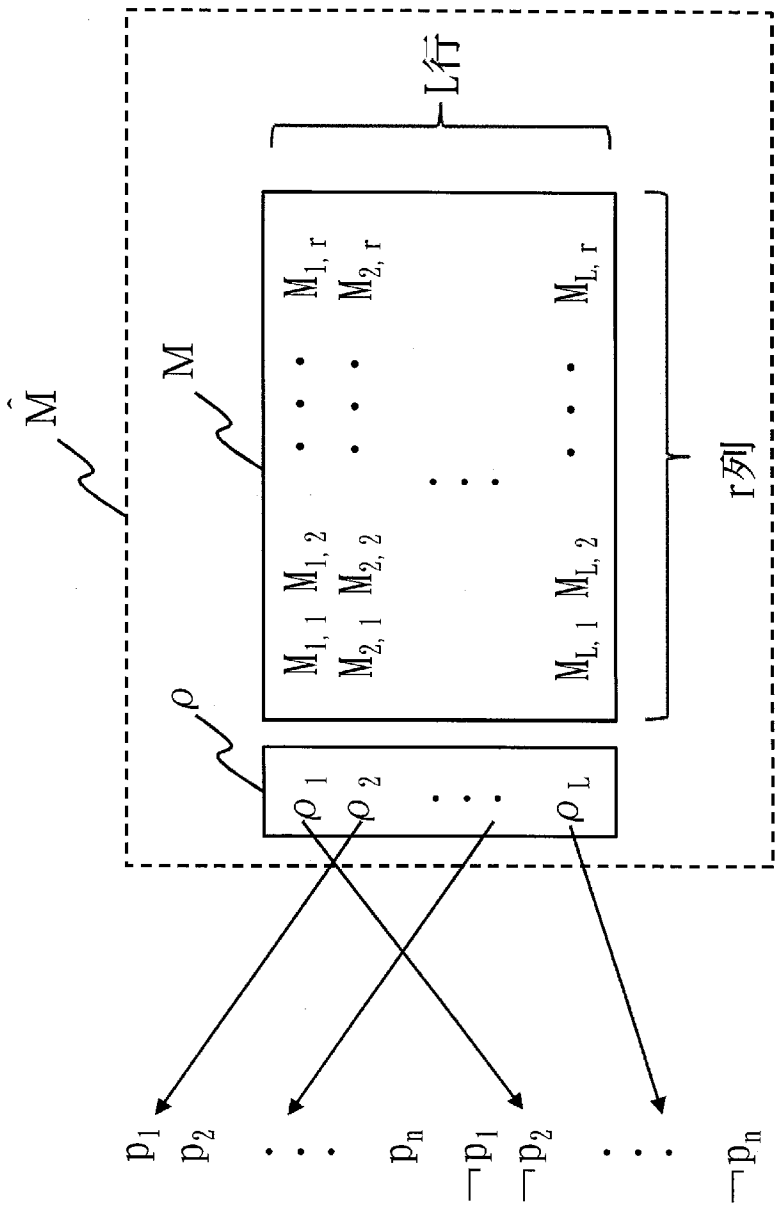
前記暗号化データｃｔ$_{(\Gamma KP,\ SCP)}$に含まれる要素c_0と要素c_t^{KP}と要素c_i^{CP}と、前記復号鍵ｓｋ$_{(SKP,\ \Gamma CP)}$に含まれる要素k^*_0と要素$k^*_i^{KP}$と要素$k^*_t^{CP}$とについて、前記ＫＰ補完係数計算処理で特定した集合I^{KP}と、前記ＫＰ補完係数計算処理で計算した補完係数α_i^{KP}と、前記ＣＰ補完係数計算処理で特定した集合I^{CP}と、前記ＣＰ補完係数計算処理で計算した補完係数α_i^{CP}とに基づき、数１に示すペアリング演算を行い値Ｋを計算するペアリング演算処理と

をコンピュータに実行させることを特徴とする暗号処理プログラム。

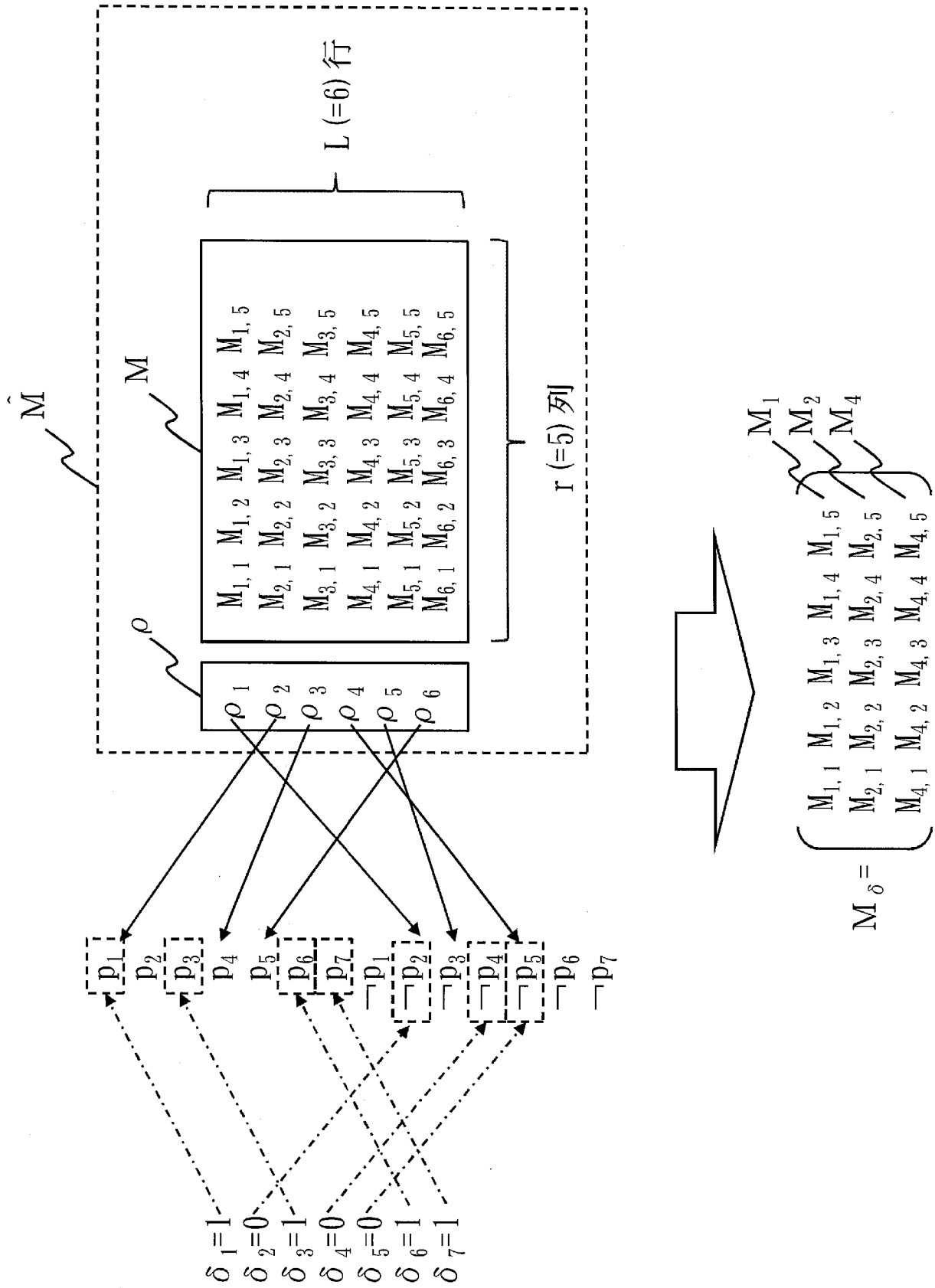
[数12]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

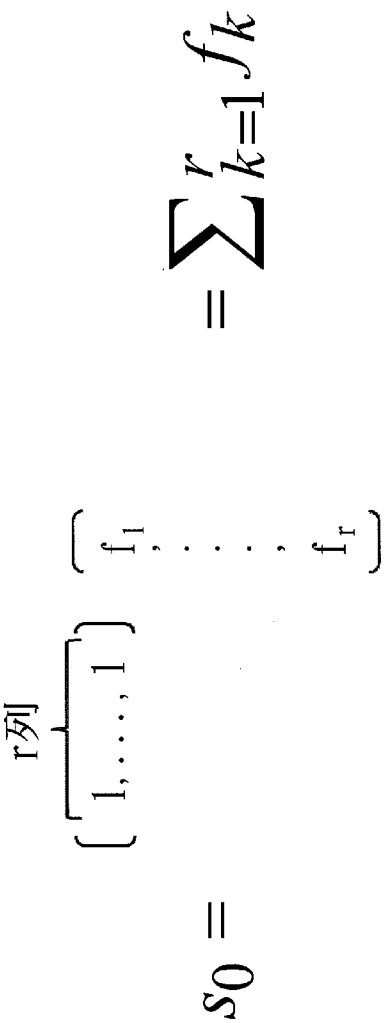
[図1]


L行
r列
M
M
ρ
ρ 1
ρ 2
ρ L
M1, 1 M1, 2 M1, r
M2, 1 M2, 2 M2, r
ML, 1 ML, 2 ML, r
p1
p2
pn
¬p1
¬p2
¬pn

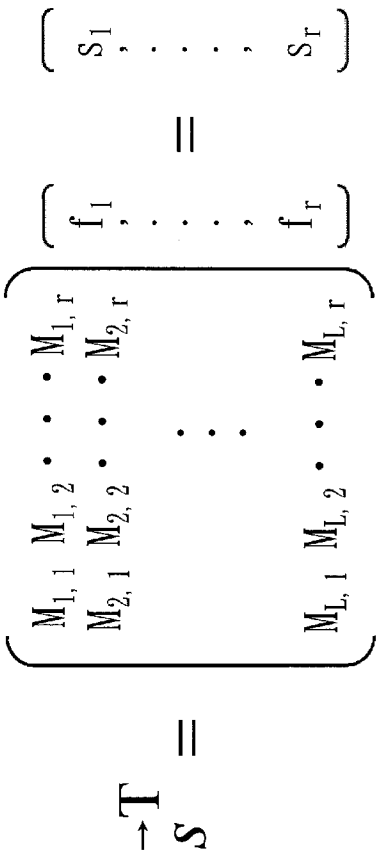
[図2]


L (=6) 行
r (=5) 列
M
ρ
p1 p2 p3 p4 p5 p6 p7 ¬p1 ¬p2 ¬p3 ¬p4 ¬p5 ¬p6 ¬p7
δ1=1 δ2=0 δ3=1 δ4=0 δ5=0 δ6=1 δ7=1
M1 M2 M4

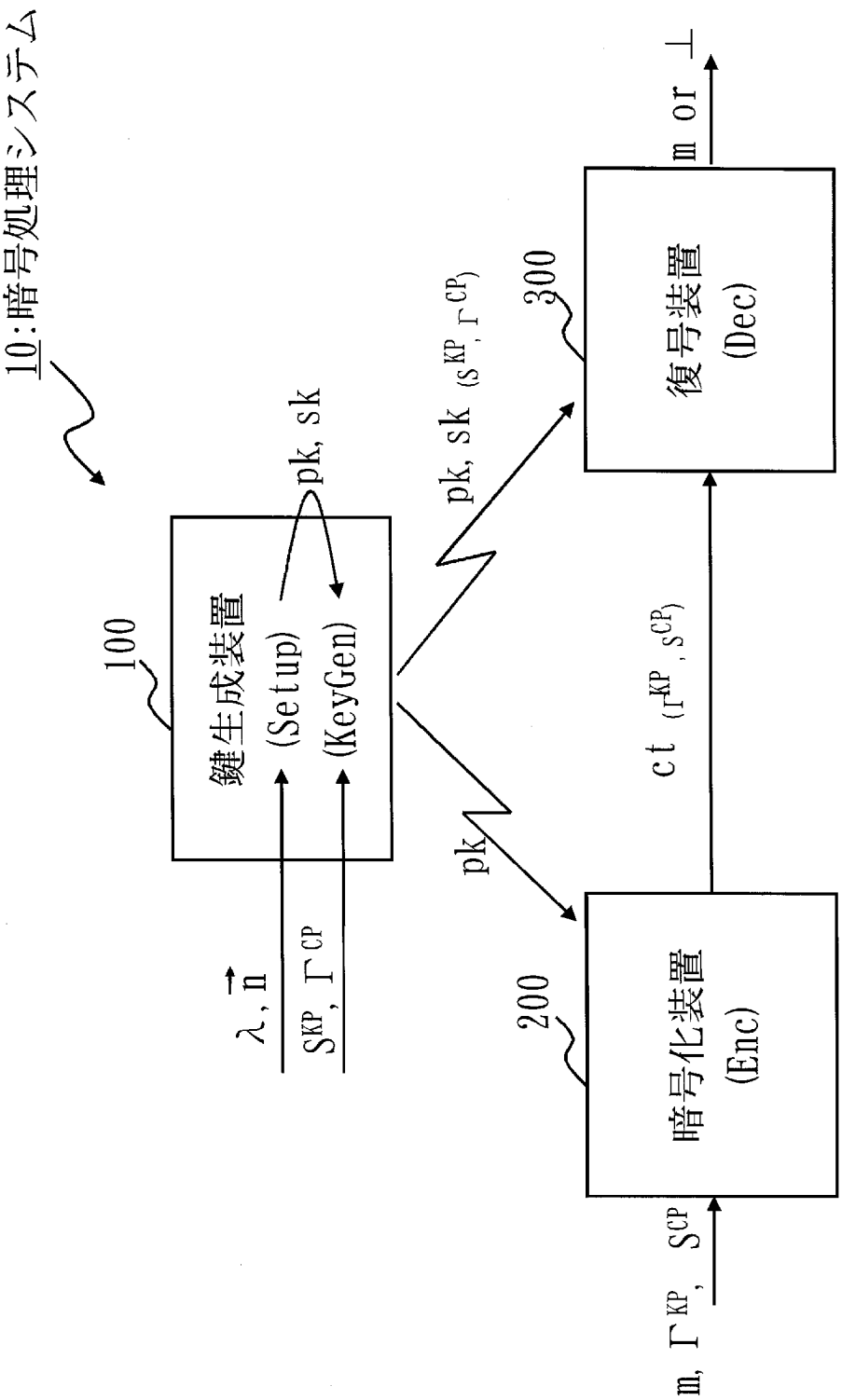
[図3]


$s_0 = \begin{pmatrix} 1, \ldots, 1 \\ \text{r列} \end{pmatrix} \begin{pmatrix} f_1, \ldots, f_r \end{pmatrix}$
$= \sum_{k=1}^{r} f_k$

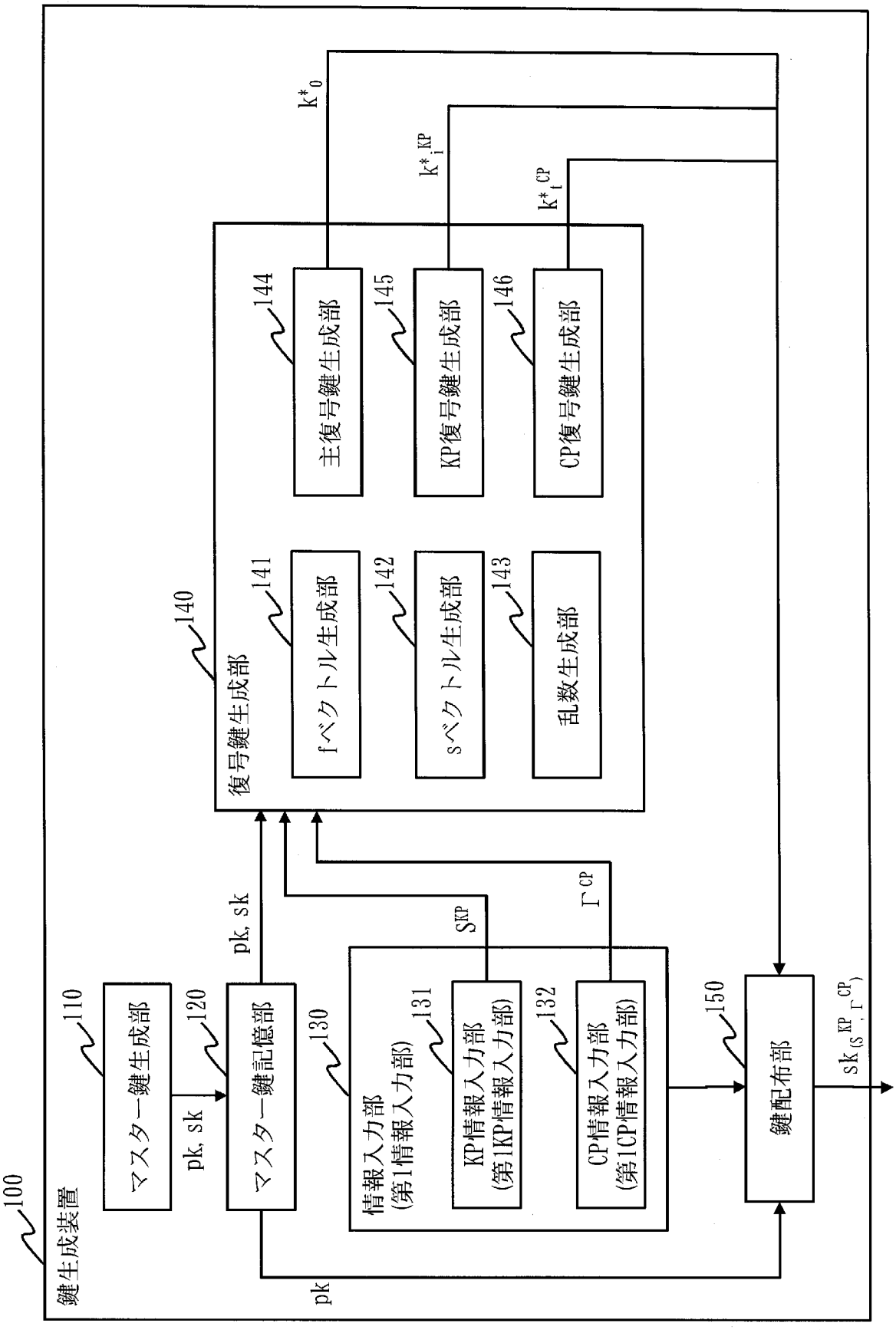
[図4]


$\vec{T}_S$
=
$\begin{pmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,r} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,r} \\ & & \cdots & \\ M_{L,1} & M_{L,2} & \cdots & M_{L,r} \end{pmatrix}$
=
$\begin{pmatrix} f_1 & , & \cdots & , & f_r \end{pmatrix}$
=
$\begin{pmatrix} S_1 & , & \cdots & , & S_r \end{pmatrix}$

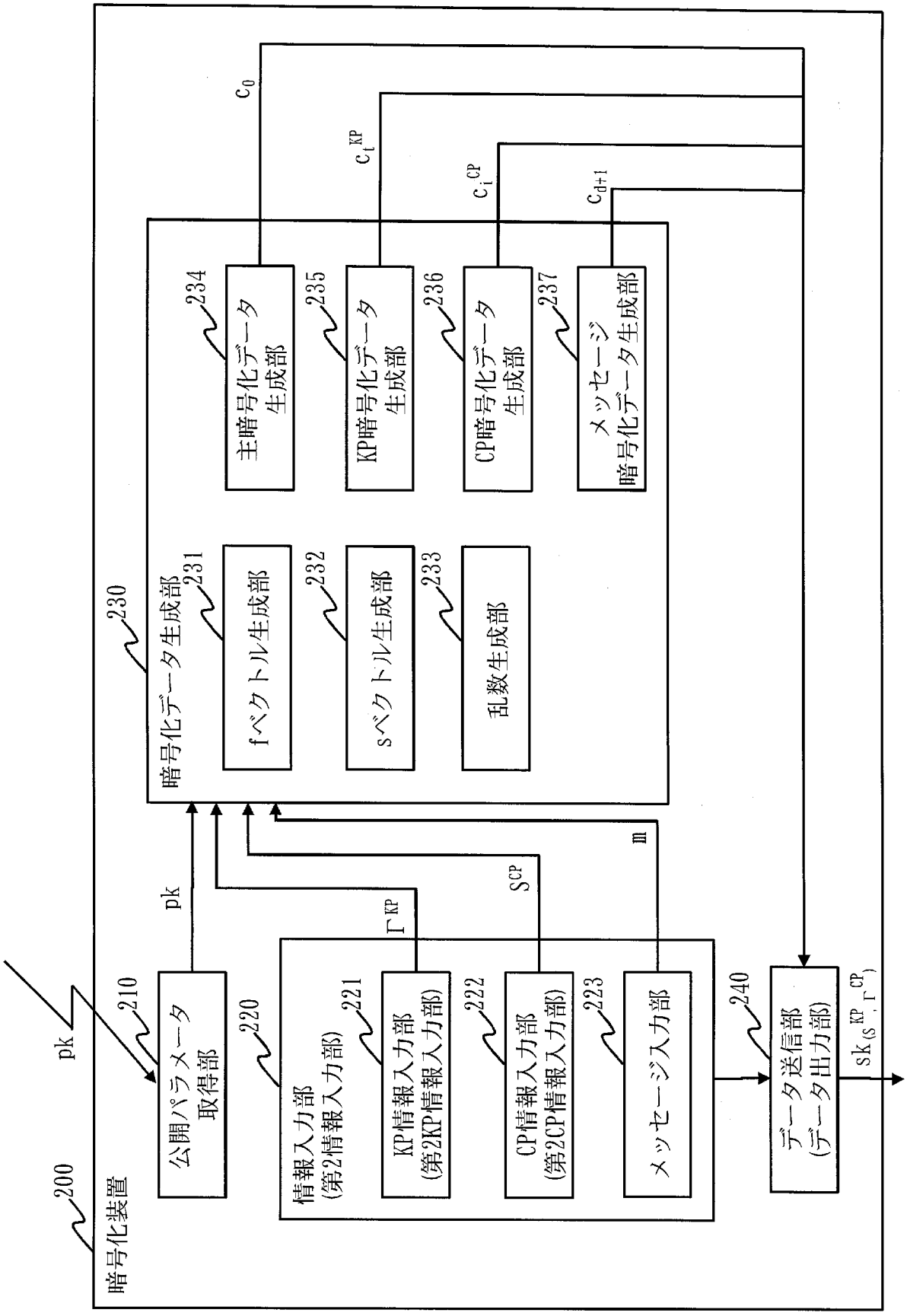
[図5]


10:暗号処理システム
100
鍵生成装置
(Setup)
(KeyGen)
pk, sk
pk, sk (S^KP, Γ^CP)
300
復号装置
(Dec)
m or ⊥
λ, n
S^KP, Γ^CP
pk
ct (Γ^KP, S^CP)
200
暗号化装置
(Enc)
m, Γ^KP, S^CP

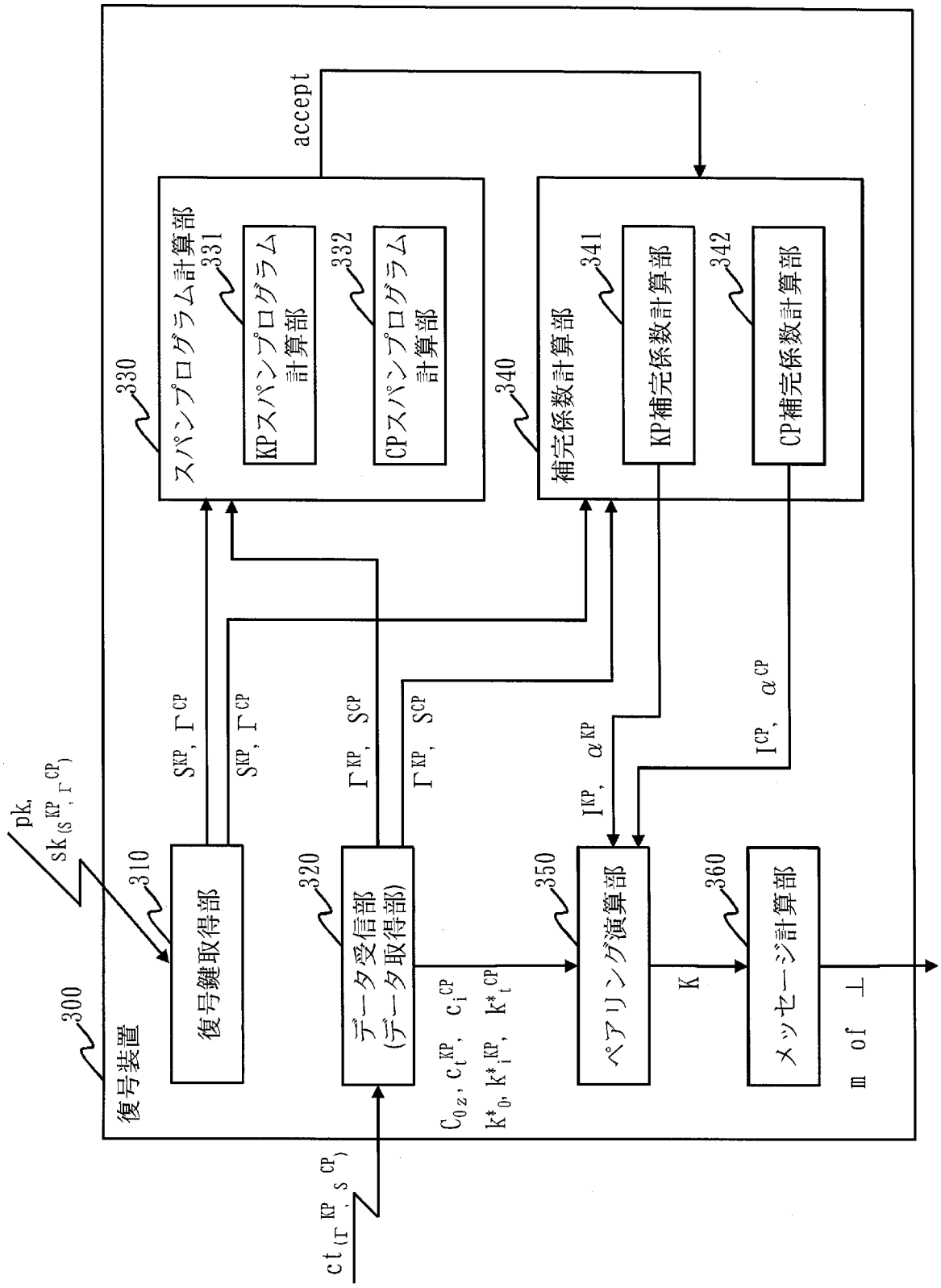
[図6]


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
(第1情報入力部)
131
KP情報入力部
(第1KP情報入力部)
132
CP情報入力部
(第1CP情報入力部)
140
復号鍵生成部
141
fベクトル生成部
142
sベクトル生成部
143
乱数生成部
144
主復号鍵生成部
145
KP復号鍵生成部
146
CP復号鍵生成部
150
鍵配布部
pk, sk
pk, sk
pk
S^{KP}
Γ^{CP}
k^*_0
k^{*KP}_i
k^{*CP}_i
$sk_{(S^{KP},\Gamma^{CP})}$

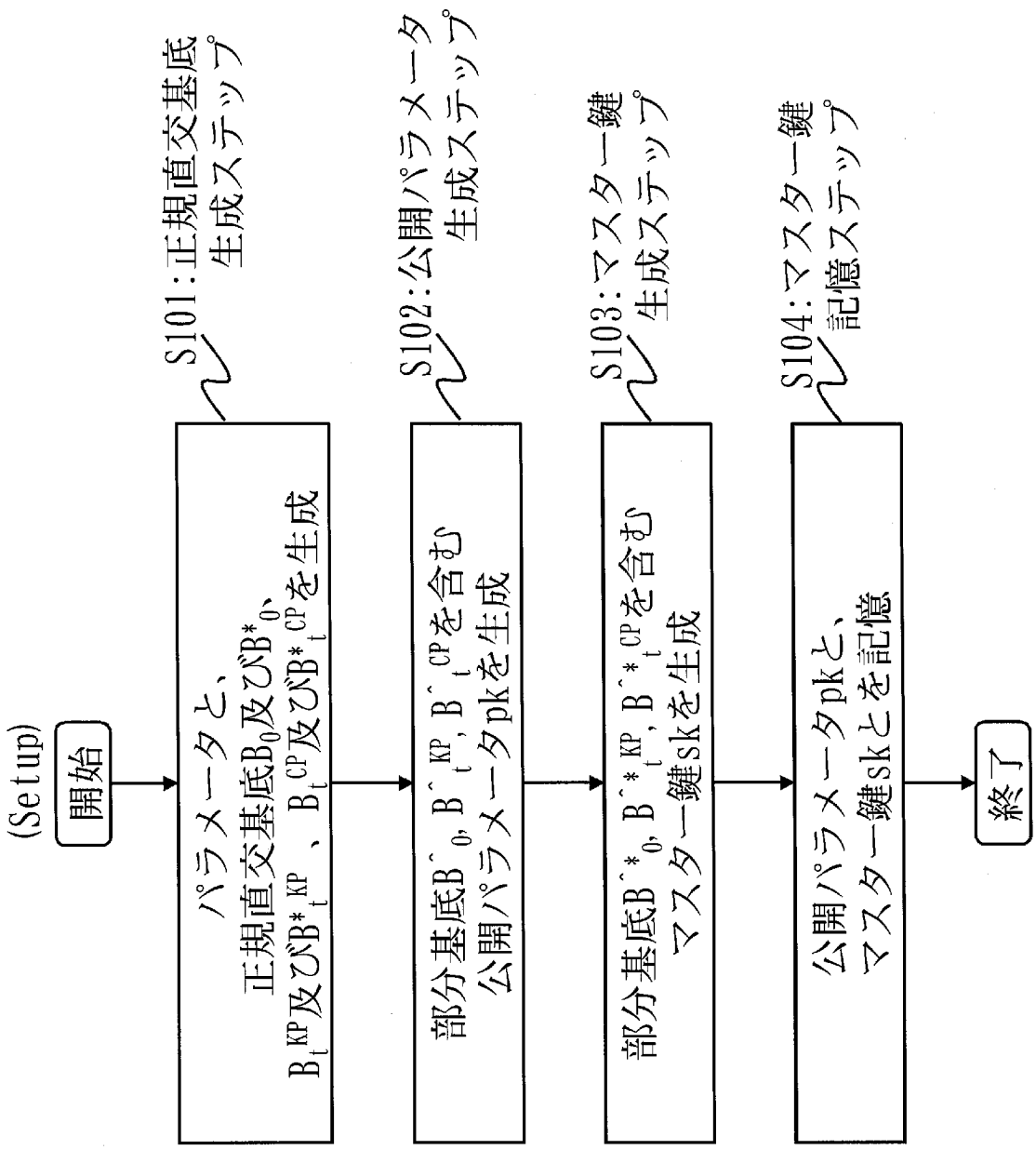
[図7]


暗号化装置
200
公開パラメータ取得部
210
情報入力部(第2情報入力部)
220
KP情報入力部(第2KP情報入力部)
221
CP情報入力部(第2CP情報入力部)
222
メッセージ入力部
223
データ送信部(データ出力部)
240
暗号化データ生成部
230
fベクトル生成部
231
sベクトル生成部
232
乱数生成部
233
主暗号化データ生成部
234
KP暗号化データ生成部
235
CP暗号化データ生成部
236
メッセージ暗号化データ生成部
237
pk
pk
Γ^{KP}
S^{CP}
m
c_0
c_t^{KP}
c_i^{CP}
c_{d+1}
$sk_{(S^{KP},\Gamma^{CP})}$

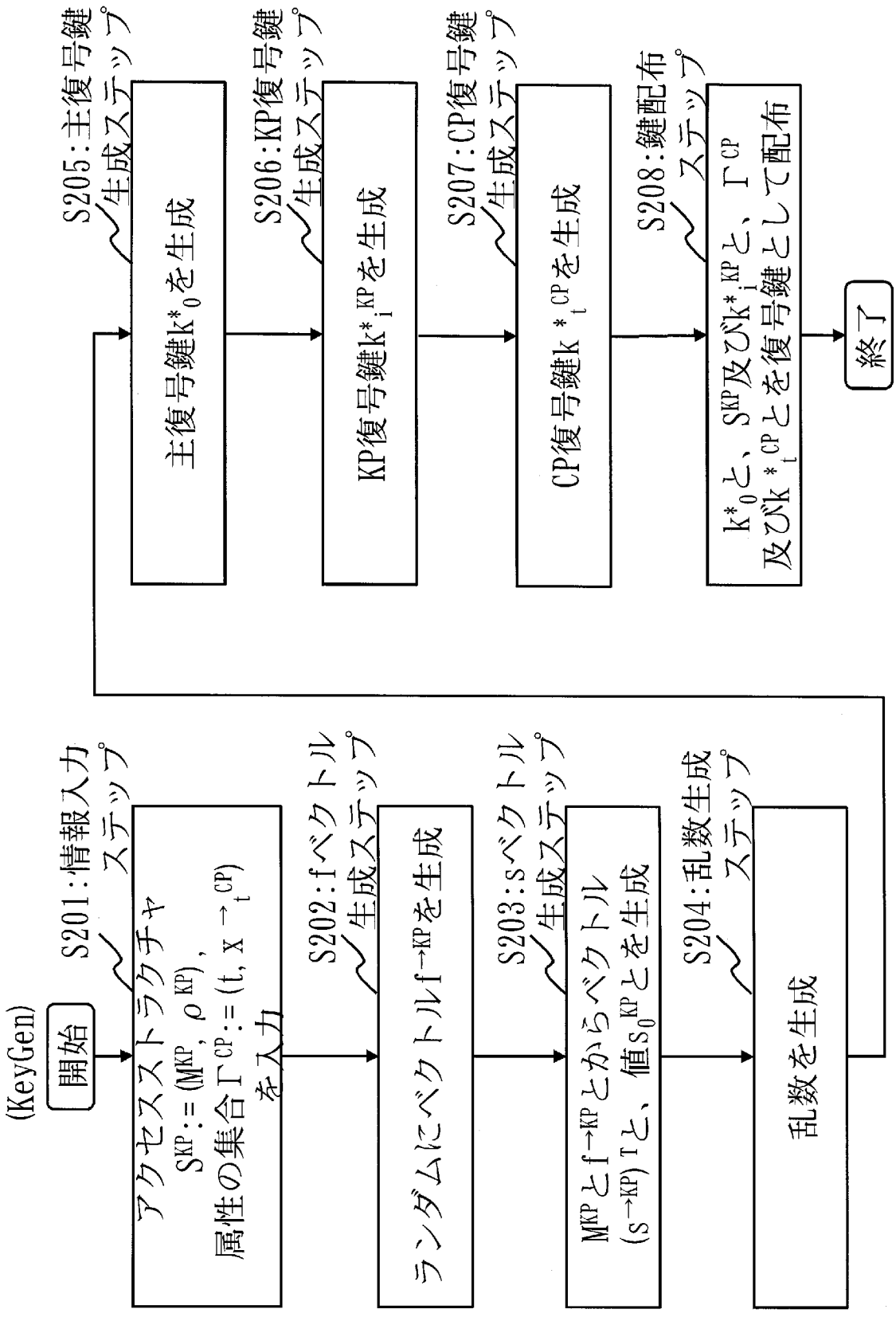
[図8]


accept
スパンプログラム計算部
330
KPスパンプログラム計算部
331
CPスパンプログラム計算部
332
補完係数計算部
340
KP補完係数計算部
341
CP補完係数計算部
342
復号装置
300
復号鍵取得部
310
データ受信部
(データ取得部)
320
ペアリング演算部
350
メッセージ計算部
360
pk,
sk(S^KP, Γ^CP)
S^KP, Γ^CP
S^KP, Γ^CP
Γ^KP, S^CP
Γ^KP, S^CP
I^KP, α^KP
I^CP, α^CP
C0z, ct^KP, ci^CP
k*0, k*i^KP, k*t^CP
K
m of ⊥
ct(Γ^KP, S^CP)

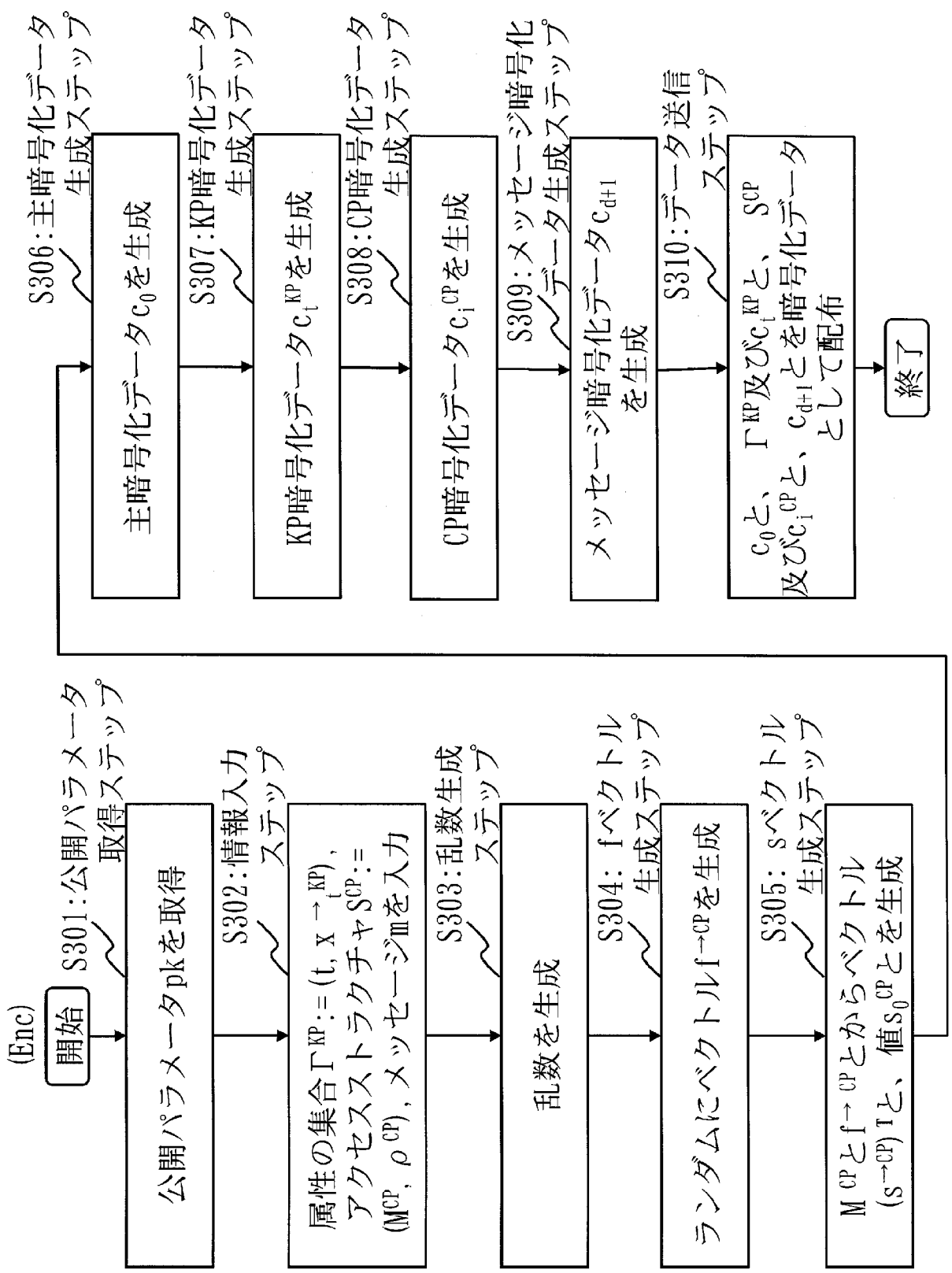
[図9]


(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_0及びB^*_0、
B_t^{KP}及び$B^{*}_t{}^{KP}$、B_t^{CP}及び$B^{*}_t{}^{CP}$を生成
S102:公開パラメータ
生成ステップ
部分基底$\hat{B}_0$, $\hat{B}_t{}^{KP}$, $\hat{B}_t{}^{CP}$を含む
公開パラメータpkを生成
S103:マスター鍵
生成ステップ
部分基底$\hat{B}^*_0$, $\hat{B}^{*}_t{}^{KP}$, $\hat{B}^{*}_t{}^{CP}$を含む
マスター鍵skを生成
S104:マスター鍵
記憶ステップ
公開パラメータpkと、
マスター鍵skとを記憶
終了

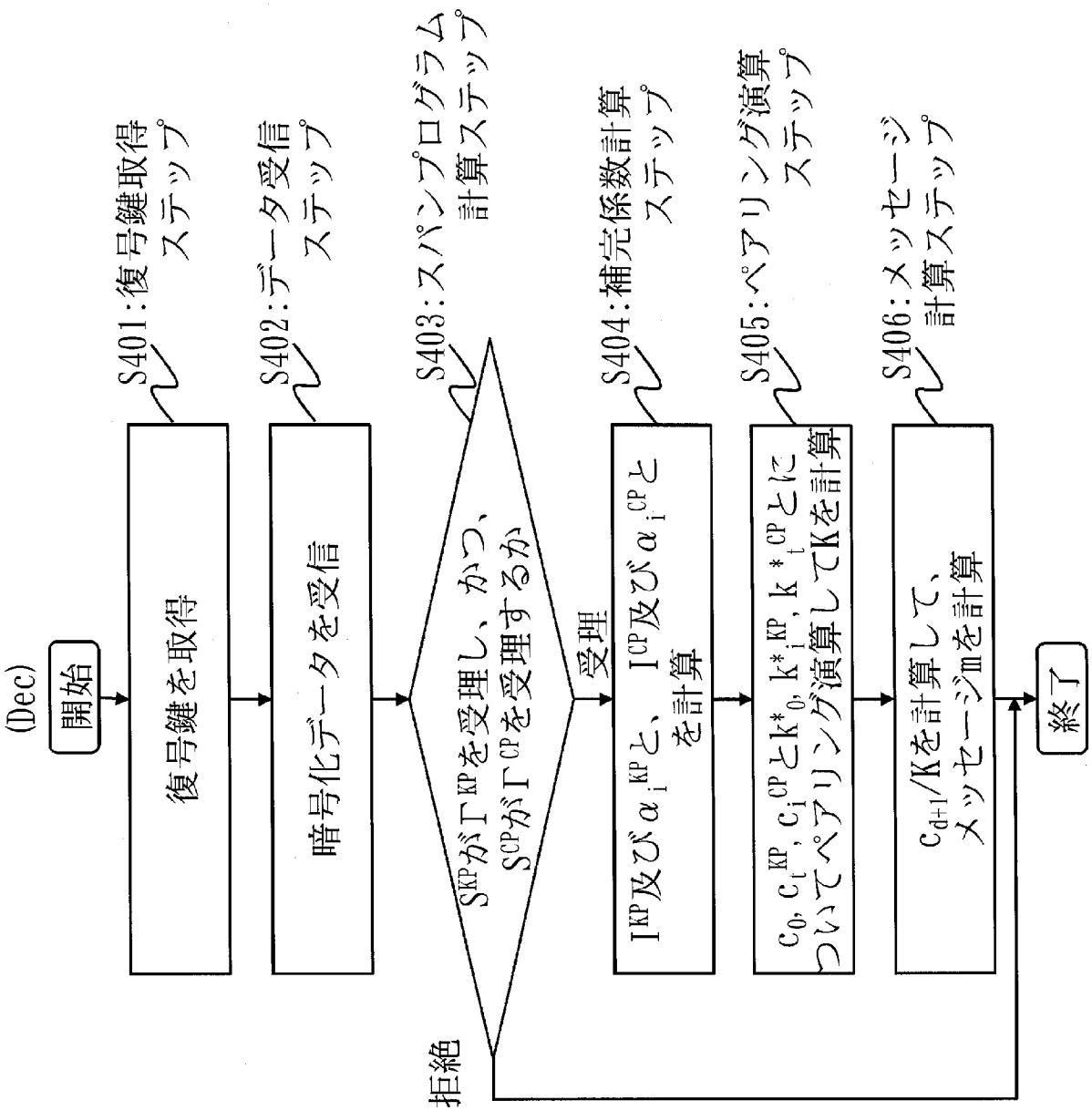
[図10]


(KeyGen)
開始
S201:情報入力ステップ
アクセスストラクチャ
$S^{KP}:=(M^{KP}, \rho^{KP})$,
属性の集合$\Gamma^{CP}:=(t, X_t^{CP})$
を入力
S202:fベクトル生成ステップ
ランダムにベクトル$f^{\to KP}$を生成
S203:sベクトル生成ステップ
M^{KP}と$f^{\to KP}$とからベクトル
$(s^{\to KP})^T$と、値s_0^{KP}とを生成
S204:乱数生成ステップ
乱数を生成
S205:主復号鍵生成ステップ
主復号鍵k^*_0を生成
S206:KP復号鍵生成ステップ
KP復号鍵$k^*_i{}^{KP}$を生成
S207:CP復号鍵生成ステップ
CP復号鍵$k^*_t{}^{CP}$を生成
S208:鍵配布ステップ
k^*_0と、S^{KP}及び$k^*_i{}^{KP}$と、Γ^{CP}
及び$k^*_t{}^{CP}$とを復号鍵として配布
終了

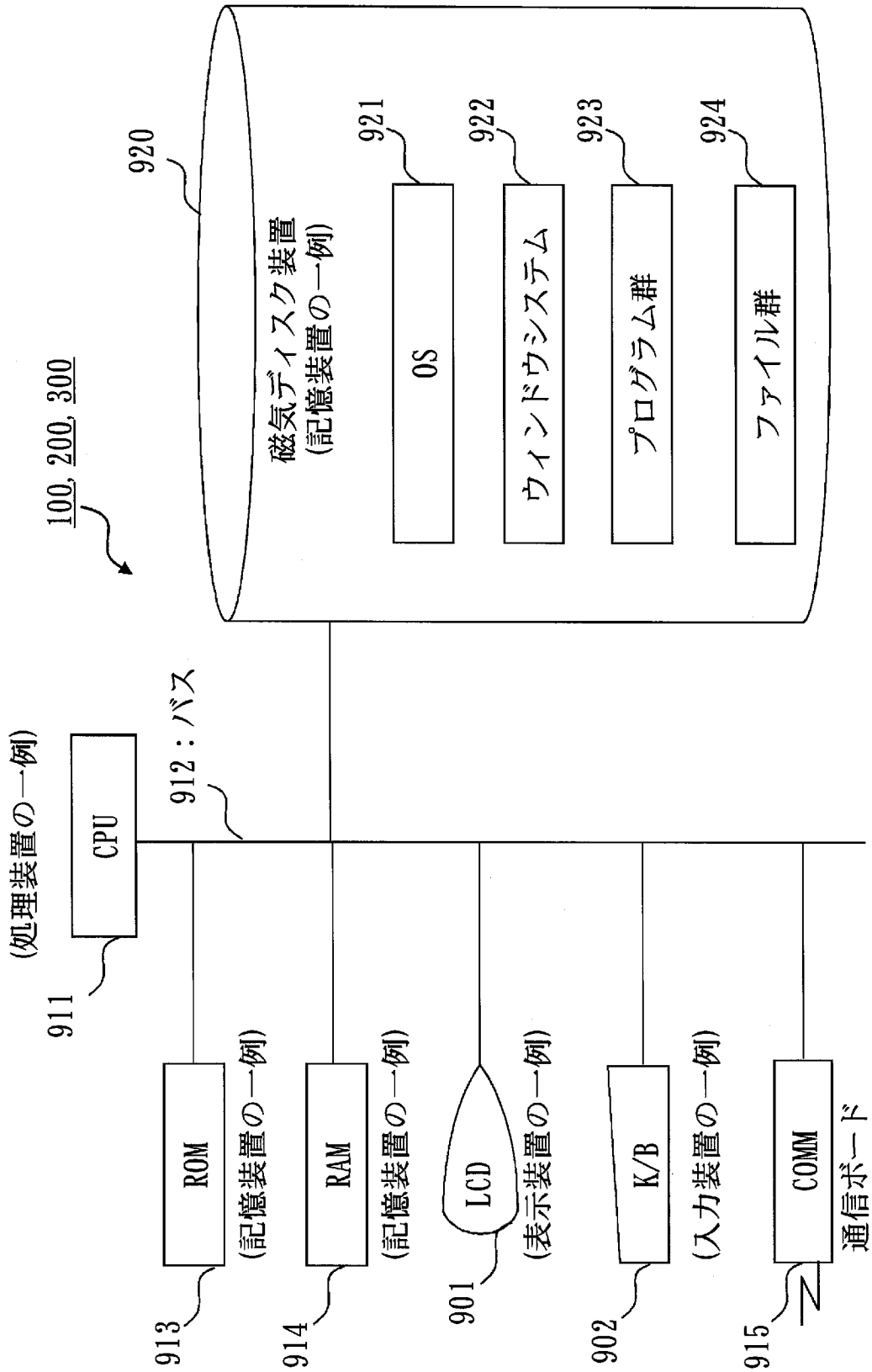
[図11]


(Enc)
開始
S301:公開パラメータ取得ステップ
公開パラメータpkを取得
S302:情報入力ステップ
属性の集合Γ^KP:=(t, X→t^KP),
アクセスストラクチャS^CP:=
(M^CP, ρ^CP), メッセージmを入力
S303:乱数生成ステップ
乱数を生成
S304: fベクトル生成ステップ
ランダムにベクトルf→^CPを生成
S305: sベクトル生成ステップ
M^CPとf→^CPとからベクトル
(s→^CP)Tと、値s0^CPとを生成
S306:主暗号化データ生成ステップ
主暗号化データc0を生成
S307:KP暗号化データ生成ステップ
KP暗号化データci^KPを生成
S308:CP暗号化データ生成ステップ
CP暗号化データci^CPを生成
S309:メッセージ暗号化データ生成ステップ
メッセージ暗号化データcd+1を生成
S310:データ送信ステップ
c0と、Γ^KP及びci^KPと、S^CP及びci^CPと、cd+1とを暗号化データとして配布
終了

[図12]


(Dec)
開始
復号鍵を取得
S401:復号鍵取得ステップ
暗号化データを受信
S402:データ受信ステップ
S403:スパンプログラム計算ステップ
S^{KP}がΓ^{KP}を受理し、かつ、S^{CP}がΓ^{CP}を受理するか
拒絶
受理
S404:補完係数計算ステップ
I^{KP}及びα_i^{KP}と、I^{CP}及びα_i^{CP}とを計算
S405:ペアリング演算ステップ
c_0, c_i^{KP}, c_i^{CP}と$k^*_0, k^{*KP}_i, k^{*CP}_i$とについてペアリング演算してKを計算
S406:メッセージ計算ステップ
c_{d+1}/Kを計算して、メッセージmを計算
終了

[図13]


100, 200, 300
920
磁気ディスク装置
(記憶装置の一例)
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
(処理装置の一例)
CPU
911
912：バス
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/JP2011/078164

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(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)
H04L9/08

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"News Analysis", THE JOURNAL OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS, 01 December 2010 (01.12.2010), vol. 93, no.12, pages 1070 to 1071	1-8
A	Nuttapong Attrapadung et al, Functional Encryption for Inner Product:Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation, 13th International Conference on Practice and Theory in Public Key Cryptography Paris, France, May 26-28, 2010 Proceedings, 2010.05, p.384-402	1-8
A	Dan Boneh et al, Functional Encryption: Definitions and Challenges, [online], 2010.11.01, Internet <http://eprint.iacr.org/cgi-bin/versions.pl?entry=2010/543>	1-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 December, 2011 (26.12.11)	10 January, 2012 (10.01.12)

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/078164

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 2011/135895 A1 (Mitsubishi Electric Corp.), 03 November 2011 (03.11.2011), entire text; all drawings (Family: none)	1-8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０７８１６４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(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.　H04L9/08

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	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１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)

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	ニュース解説，電子情報通信学会誌　第９３巻　第１２号　THE JOURNAL OF THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS, 2010.12.01, 第93巻　第12号, p.1070-1071	１－８

☑　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 ２６．１２．２０１１	国際調査報告の発送日 １０．０１．２０１２
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　３１４６ 松平　英 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Ａ	Nuttapong Attrapadung et al, Functional Encryption for Inner Product:Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation, 13th International Conference on Practice and Theory in Public Key Cryptography Paris, France, May 26-28, 2010 Proceedings, 2010.05, p.384-402	１－８
Ａ	Dan Boneh et al, Functional Encryption:Definitions and Challenges, [online], 2010.11.01, インターネット <http://eprint.iacr.org/cgi-bin/versions.pl?entry=2010/543>	１－８
Ｐ，Ａ	WO 2011/135895 A1 (三菱電機株式会社) 2011.11.03, 全文, 全図 (ファミリーなし)	１－８