(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
2010 年 10 月 28 日(28.10.2010)

PCT

(10) 国際公開番号
WO 2010/123116 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2010/057279

(22) 国際出願日: 2010 年 4 月 23 日(23.04.2010)

(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 2009-106009 2009 年 4 月 24 日(24.04.2009) JP

(71) 出願人 (米国を除く全ての指定国について): 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): 鈴木 幸太郎(SUZUKI, Koutarou) [JP/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). 西巻 陵(NISHIMAKI, Ryo) [JP/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: 中尾 直樹, 外(NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル４階 Tokyo (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, JP, 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, RO, RS, RU, 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, 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 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,

[続葉有]

(54) **Title**: INFORMATION GENERATING DEVICE, INFORMATION GENERATING METHOD, AND INFORMATION GENERATING PROGRAM AND STORAGE MEDIUM THEREOF

(54) 発明の名称 : 情報生成装置、方法、プログラム及びその記録媒体

[図1]

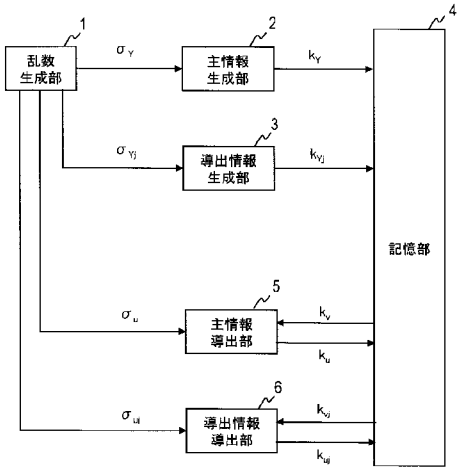

図1

1 RANDOM-NUMBER GENERATING UNIT
2 MAIN-INFORMATION GENERATING UNIT
3 DERIVATION-INFORMATION GENERATING UNIT
4 STORAGE UNIT
5 MAIN-INFORMATION DERIVING UNIT
6 DERIVATION-INFORMATION DERIVING UNIT

(57) **Abstract**: A hierarchy type cryptogram, to be indicated by a generic partial-order structure other than a tree structure, will be achieved. In generating information, random numbers σ_v, $(\sigma_{vj})_{j\in w(v)} \in Z_q$ are generated, main information $k_v=\sigma_v \Sigma_{i\in[1,\cdots,N-1]\setminus w(v)} v_i b_i^* + b_N^*$ is calculated, and derivation information $k_{vj}=\sigma_{vj} \Sigma_{i\in[1,\cdots,N-1]\setminus w(v)} v_i b_i^* + b_j^*$ is calculated for each $j \in w(v)$. In deriving information, random numbers σ_u, $(\sigma_{uj})_{j\in w(u)} \in Z_q$ are generated, main information $k_u=\sigma_u \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_v$ is calculated, and derivation information $k_{uj}=\sigma_{uj} \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_{vj}$ is calculated for each $j \in w(u)$.

(57) 要約: 木構造以外の一般の半順序構造で表される階層型暗号を実現する。情報生成においては、乱数σ_v, $(\sigma_{vj})_{j\in w(v)} \in Z_q$を生成し、主情報$k_v=\sigma_v \Sigma_{i\in[1,\cdots,N-1]\setminus w(v)} v_i b_i^* + b_N^*$を計算し、各$j \in w(v)$について導出情報$k_{vj}=\sigma_{vj} \Sigma_{i\in[1,\cdots,N-1]\setminus w(v)} v_i b_i^* + b_j^*$を計算する。情報導出においては、乱数$\sigma_u$, $(\sigma_{uj})_{j\in w(u)} \in Z_q$を生成し、主情報$k_u=\sigma_u \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_v$を計算し、各$j \in w(u)$について導出情報$k_{uj}=\sigma_{uj} \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_{vj}$を計算する。

WO 2010/123116 A1

GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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 ： 情報生成装置、方法、プログラム及びその記録媒体

技術分野

[0001] この発明は、情報セキュリティ技術の応用技術に関する。例えば、復号鍵からより復号権限の制限された復号鍵を導出することができる階層型暗号に関するものである。

背景技術

[0002] 階層型暗号の従来技術として、非特許文献１に記載された技術が知られている。

先行技術文献

非特許文献

[0003] 非特許文献1：Craig Gentry, Alice Silverberg, “Hierarchical ID-Based Cryptography”, ASIACRYPT 2002, p.548-566

発明の概要

発明が解決しようとする課題

[0004] 非特許文献１に記載された技術では、木構造の親ノードに対応する鍵から子ノードに対応する鍵を導出することはできるが、木構造以外の一般の半順序構造ｓで表される鍵導出を実現することはできなかった。例えば、共通の子ノードＣを持つ親ノードＡと親ノードＢに対して、親ノードＡの鍵から共通の子ノードＣの鍵を導出し、親ノードＢの鍵から共通の子ノードＣの鍵を導出することはできないという課題があった。

課題を解決するための手段

[0005] 上記の課題を解決するために、請求項１の情報生成装置は、ｅが巡回群G_1のＮ個の元g_L（Ｌ＝１，…，Ｎ）（Ｎ≧２）と巡回群G_2のＮ個の元g_L^*（Ｌ＝１，…，Ｎ）との入力に対して巡回群G_Tの１個の元を出力する非退化な双線形関数であり、$b_i \in G_1^N$（ｉ＝１，…，Ｎ）のそれぞれが、上記巡回群G_1のＮ個の元を要素とするＮ次元の基底ベクトルであり、$b_j^* \in G_2^N$（ｊ＝

１，…，Ｎ）のそれぞれが、上記巡回群$Ｇ_2$のＮ個の元を要素とするＮ次元の基底ベクトルであり、上記基底ベクトル$ｂ_ｉ∈Ｇ_1^Ｎ$（ｉ＝１，…，Ｎ）の各要素と上記基底ベクトル$ｂ_ｊ*∈Ｇ_2^Ｎ$（ｊ＝１，…，Ｎ）の各要素とを上記双線形関数ｅに入力して得られる関数値が、ｉ＝ｊの場合に$δ（ｉ，ｊ）＝１_Ｆ$となってｉ≠ｊの場合に$δ（ｉ，ｊ）＝０_Ｆ$となるクロネッカーのデルタ関数δ（ｉ，ｊ）を用いて$ｇ_Ｔ^{τ・δ（ｉ，ｊ）}∈Ｇ_Ｔ$と表現され、$０_Ｆ$が有限体$Ｆ_ｑ$の加法単位元であり、$１_Ｆ$が有限体$Ｆ_ｑ$の乗法単位元であり、τが$０_Ｆ$を除く有限体$Ｆ_ｑ$の元であり、$ｇ_Ｔ$が上記巡回群$Ｇ_Ｔ$の生成元であり、＊を不定文字とし、インデックスＹをＹ＝（$Ｙ_1$，…，$Ｙ_{Ｎ－1}$）∈Ｉ＝（$Ｆ_ｑ$∪｛＊｝）$^{Ｎ－1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜$Ｙ_ｉ$＝＊｝として、乱数$σ_Ｙ∈Ｚ_ｑ$、及び、集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）に対応する乱数$σ_{Ｙｊ}∈Ｚ_ｑ$を生成する乱数生成部と、上記生成された乱数$σ_Ｙ$を用いて、$ｋ_Ｙ＝σ_Ｙ Σ_{ｉ∈｛1，…，Ｎ－1｝＼ｗ（Ｙ）} Ｙ_ｉ ｂ_ｉ*＋ｂ_Ｎ*$の関係を満たす主情報$ｋ_Ｙ$を計算する主情報生成部と、上記生成された乱数$σ_{Ｙｊ}$を用いて、$ｋ_{Ｙｊ}＝σ_{Ｙｊ} Σ_{ｉ∈｛1，…，Ｎ－1｝＼ｗ（Ｙ）} Ｙ_ｉ ｂ_ｉ*＋ｂ_ｊ*$の関係を満たす導出情報$ｋ_{Ｙｊ}$を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）ごとに計算する導出情報生成部と、を含む。

[0006] 請求項４の情報生成装置は、ｅが巡回群$Ｇ_1$のＮ個の元$γ_Ｌ$（Ｌ＝１，…，Ｎ）（Ｎ≧２）と巡回群$Ｇ_2$のＮ個の元$γ_Ｌ*$（Ｌ＝１，…，Ｎ）との入力に対して巡回群$Ｇ_Ｔ$の１個の元を出力する非退化な双線形関数であり、$ｂ_ｉ∈Ｇ_1^Ｎ$（ｉ＝１，…，Ｎ）のそれぞれが、上記巡回群$Ｇ_1$のＮ個の元を要素とするＮ次元の基底ベクトルであり、$ｂ_ｊ*∈Ｇ_2^Ｎ$（ｊ＝１，…，Ｎ）のそれぞれが、上記巡回群$Ｇ_2$のＮ個の元を要素とするＮ次元の基底ベクトルであり、上記基底ベクトル$ｂ_ｉ∈Ｇ_1^Ｎ$（ｉ＝１，…，Ｎ）の各要素と上記基底ベクトル$ｂ_ｊ*∈Ｇ_2^Ｎ$（ｊ＝１，…，Ｎ）の各要素とを上記双線形関数ｅに入力して得られる関数値が、ｉ＝ｊの場合に$δ（ｉ，ｊ）＝１_Ｆ$となってｉ≠ｊの場合に$δ（ｉ，ｊ）＝０_Ｆ$となるクロネッカーのデルタ関数δ（ｉ，ｊ）を用いて$ｇ_Ｔ^{τ・δ（ｉ，ｊ）}∈Ｇ_Ｔ$と表現され、$０_Ｆ$が有限体$Ｆ_ｑ$の加法単位元であり、$１_Ｆ$が有限体$Ｆ_ｑ$の乗法単位元であり、τが$０_Ｆ$を除く有限体$Ｆ_ｑ$の元であり、$ｇ_Ｔ$が上記巡回

群G_Tの生成元であり、＊を不定文字とし、インデックスＹをＹ＝（Y_1，…，Y_{N-1}）∈Ｉ＝（F_qＵ｛＊｝）$^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜Y_i＝＊｝とし、$\sigma_Y \in Z_q$を乱数とし、σ_{Yi}を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）に対応する乱数とし、インデックスＹに対応する主情報k_Yは$k_Y=\sigma_Y \Sigma_{i\in\{1,\cdots,N-1\}\setminus w(Y)} Y_i b_i^* + b_N^*$の関係を満たし、インデックスＹに対応する導出情報$k_{Yi}$は$k_{Yj}=\sigma_{Yj} \Sigma_{i\in\{1,\cdots,N-1\}\setminus w(Y)} Y_i b_i^* + b_j^*$の関係を満たし、＊を不定文字とし、インデックスｖをｖ＝（v_1，…，v_{N-1}）∈Ｉ＝（F_qＵ｛＊｝）$^{N-1}$とし、インデックスｕをｕ＝（u_1，…，u_{N-1}）∈Ｉ＝（F_qＵ｛＊｝）$^{N-1}$とし、インデックスｖに対応する集合ｗ（ｖ）をｗ（ｖ）＝｛ｉ｜v_i＝＊｝とし、インデックスｕに対応する集合ｗ（ｕ）をｗ（ｕ）＝｛ｉ｜u_i＝＊｝とし、集合ｗ（ｕ）⊂集合ｗ（ｖ）とし、$v_i=u_i$（ｉ∈｛１，…，Ｎ－１｝＼ｗ（ｖ））として、上記主情報k_Yである又は上記主情報k_Y及び上記導出情報k_{Yi}から導出されたインデックスｖに対応する主情報k_v、及び、上記導出情報k_{Yi}である又は上記導出情報k_{Yi}から導出されたインデックスｖに対応する導出情報k_{vj}を記憶する記憶部と、乱数$\sigma_u \in Z_q$を生成する子乱数生成部と、上記記憶部から読み込んだ主情報k_v、導出情報k_{vi}及び上記生成された乱数σ_uを用いて、$k_u=\sigma_u \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_v$の関係を満たす、インデックスｕに対応する主情報$k_u$を計算する主情報導出部と、を含む。

[0007] 請求項６の情報生成装置は、Ｇ、G_Tを素数位数ｑの巡回群とし、ｇを巡回群Ｇの生成元とし、巡回群Ｇには$g_T=e(g,g)$が巡回群G_Tの生成元となるようなペアリング関数ｅ：Ｇ×Ｇ→G_Tが存在するとし、ａをZ_pからランダムに選択された乱数とし、ｇと$g_1=g^a \in G$と巡回群Ｇからランダムに選択されたg_2，g_3，h_1，…，$h_{N-1} \in G$とが公開鍵として公開されており、＊を不定文字とし、インデックスＹをＹ＝（Y_1，…，Y_{N-1}）∈Ｉ＝（F_qＵ｛＊｝）$^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜Y_i＝＊｝として、乱数$r_Y \in Z_q$を生成する乱数生成部と、上記生成された乱数r_Yを用いて、$k_Y=g_2^a (g_3 \Pi_{i\in\{1,\cdots,N-1\}\setminus w(Y)} h_i^{Yi})^{r_Y}$の関

係を満たす第一主情報k_Yを計算する第一主情報生成部と、上記生成された乱数r_Yを用いて、第二主情報g^{r_Y}を計算する第二主情報生成部と、上記生成された乱数r_Yを用いて、$k_{Yj}=h_j^{r_Y}$の関係を満たす導出情報k_{Yj}を集合w（Y）の各要素$j\in w(Y)$ごとに計算する導出情報生成部と、を含む。

[0008] 請求項９の情報生成装置は、G、G_Tを素数位数qの巡回群とし、gを巡回群Gの生成元とし、巡回群Gには$g_T=e(g, g)$が巡回群G_Tの生成元となるようなペアリング関数$e: G\times G\rightarrow G_T$が存在するとし、aを$Z_p$からランダムに選択された乱数とし、gと$g_1=g^a\in G$と巡回群Gからランダムに選択された$g_2, g_3, h_1, \cdots, h_{N-1}\in G$とが公開鍵として公開されており、＊を不定文字とし、インデックスYを$Y=(Y_1, \cdots, Y_{N-1})\in I=(F_q\cup\{*\})^{N-1}$とし、インデックスYに対応する集合w（Y）をw（Y）＝｛i｜$Y_i=*$｝とし、$r_Y\in Z_q$を乱数とし、インデックスYに対応する第一主情報k_Yは$k_Y=g_2^a(g_3\prod_{i\in[1,\cdots,N-1]\setminus w(Y)}h_i^{Y_i})^{r_Y}$の関係を満たし、$g^{r_Y}$をインデックスYに対応する第二主情報とし、インデックスYに対応する導出情報k_{Yi}は$k_{Yj}=h_j^{r_Y}$の関係を満たし、＊を不定文字とし、インデックスvを$v=(v_1, \cdots, v_{N-1})\in I=(F_q\cup\{*\})^{N-1}$とし、インデックスvに対応する集合w（v）をw（v）＝｛i｜$v_i=*$｝とし、インデックスuを$u=(u_1, \cdots, u_{N-1})\in I=(F_q\cup\{*\})^{N-1}$とし、インデックスuに対応する集合w（u）をw（u）＝｛i｜$u_i=*$｝とし、集合w（u）⊂集合w（v）とし、$v_i=u_i$（$i\in\{1, \cdots, N-1\}\setminus w(v)$）として、乱数$r_u\in Z_q$を生成する乱数生成部と、上記第一主情報$k_Y$である又は上記第一主情報$k_Y$及び上記導出情報$k_{Yi}$から導出されたインデックスvに対応する第一主情報$k_v$、上記導出情報$k_{Yi}$である又は上記導出情報$k_{Yi}$から導出されたインデックスvに対応する導出情報$k_{vj}$を記憶する記憶部と、上記記憶部から読み込んだ第一主情報k_v及び上記導出情報k_{vi}を用いて、$k_u=k_v(\prod_{i\in w(v)\setminus w(u)}k_{vi}^{u_i})(g_3\prod_{i\in[1,\cdots,N-1]\setminus w(v)}h_i^{v_i}\prod_{i\in w(v)\setminus w(u)}h_i^{u_i})^{r_u}$の関係を満たす、インデックスuに対応する第一主情報k_uを計算する第一主情報導出部と、上記生成された乱数r_uを用いて、第

二主情報g^{ru}を計算する第二主情報導出部と、を含む。

発明の効果

[0009] 共通の子ノードCを持つ親ノードAと親ノードBに対して、親ノードAの情報から共通の子ノードCの情報を導出し、親ノードBの情報から共通の子ノードCの情報を導出することができる。

図面の簡単な説明

[0010] [図1]第一実施形態の情報生成装置の機能ブロック図の例。

[図2]第一実施形態の情報生成のフローチャートの例。

[図3]第一実施形態の情報導出のフローチャートの例。

[図4]第二実施形態の情報生成装置の機能ブロック図の例。

[図5]第二実施形態の情報生成のフローチャートの例。

[図6]第二実施形態の情報導出のフローチャートの例。

発明を実施するための形態

[0011] 以下、この発明の実施の形態について、詳細に説明する。

［述語暗号］

まず、第一実施形態で用いる概念である述語暗号の概要について説明する。

[0012] 〔定義〕

まず、本形態で使用する用語や記号を定義する。

行列：「行列」とは演算が定義された集合の元を矩形に並べたものを表す。環の元を要素とするものだけではなく、群の元を要素とするものも「行列」と表現する。

[0013] $(\cdot)^{T}$：$(\cdot)^{T}$は・の転置行列を表す。

$(\cdot)^{-1}$：$(\cdot)^{-1}$は・の逆行列を表す。

∧：∧は論理積を表す。

∨：∨は論理和を表す。

Ｚ：Ｚは整数集合を表す。

ｋ：ｋはセキュリティパラメータ（$k\in Z,\ k>0$）を表す。

[0014] $\{0,1\}^*$：$\{0,1\}^*$は任意ビット長のバイナリ系列を表す。その一例は、整数0及び1からなる系列である。しかし、$\{0,1\}^*$は整数0及び1からなる系列に限定されない。$\{0,1\}^*$は位数2の有限体又はその拡大体と同義である。

$\{0,1\}^\zeta$：$\{0,1\}^\zeta$はビット長ζ（$\zeta \in Z$, $\zeta>0$）のバイナリ系列を表す。その一例は、整数0及び1からなる系列である。しかし、$\{0,1\}^\zeta$は整数0及び1からなる系列に限定されない。$\{0,1\}^\zeta$は位数2の有限体（$\zeta=1$の場合）又はそれをζ次拡大した拡大体（$\zeta>1$の場合）と同義である。

(+)：(+)はバイナリ系列間の排他的論理和演算子を表す。例えば、10110011 (+) 11100001=01010010を満たす。

[0015] F_q：F_qは位数qの有限体を表す。位数qは１以上の整数であり、例えば、素数や素数のべき乗値を位数qとする。すなわち、有限体F_qの例は素体やそれを基礎体とした拡大体である。なお、有限体F_qが素体である場合の演算は、例えば、位数qを法とする剰余演算によって容易に構成できる。また、有限体F_qが拡大体である場合の演算は、例えば、既約多項式を法とする剰余演算によって容易に構成できる。有限体F_qの具体的な構成方法は、例えば、参考文献１「ISO/IEC 18033-2: Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers」に開示されている。

[0016] 0_F：0_Fは有限体F_qの加法単位元を表す。

1_F：1_Fは有限体F_qの乗法単位元を表す。

$\delta(i,j)$：$\delta(i,j)$はクロネッカーのデルタ関数を表す。i=jの場合に$\delta(i,j)=1_F$を満たし、i≠jの場合に$\delta(i,j)=0_F$を満たす。

E：Eは有限体F_q上で定義された楕円曲線を表す。Eはアフィン（affine）座標版のWeierstrass方程式

$$y^2+a_1 \cdot x \cdot y+a_3 \cdot y=x^3+a_2 \cdot x^2+a_4 \cdot x+a_6 \quad \cdots(1)$$

（ただし、$a_1, a_2, a_3, a_4, a_6 \in F_q$）を満たすx, y$\in F_q$からなる点(x,y)の集合に無限遠点と呼ばれる特別な点Oを付加したもので定義される。楕円曲線E上の任意の２点に対して楕円加算と呼ばれる二項演算＋及び楕円曲線E上の任意の１点に対して楕円逆元と呼ばれる単項演算－がそれぞれ定義できる。また、楕円

曲線E上の有理点からなる有限集合が楕円加算に関して群をなすこと、楕円加算を用いて楕円スカラー倍算と呼ばれる演算が定義できること、及びコンピュータ上での楕円加算などの楕円演算の具体的な演算方法はよく知られている（例えば、参考文献１、参考文献２「RFC 5091: Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems」、参考文献３「イアン・Ｆ・ブラケ、ガディエル・セロッシ、ナイジェル・Ｐ・スマート＝著、「楕円曲線暗号」、出版＝ピアソン・エデュケーション、ISBN4-89471-431-0」等参照）。

[0017] また、楕円曲線E上の有理点からなる有限集合は位数p(p≧1)の部分群を持つ。例えば、楕円曲線E上の有理点からなる有限集合の要素数を#Eとし、pを#Eを割り切る大きい素数とした場合、楕円曲線Eのp等分点からなる有限集合E[p]は、楕円曲線E上の有理点からなる有限集合の部分群を構成する。なお、楕円曲線Eのp等分点とは、楕円曲線E上の点Aのうち、楕円曲線E上での楕円スカラー倍算値p・Aがp・A＝Ｏを満たす点を意味する。

[0018] G_1, G_2, G_T：G_1, G_2, G_Tは位数qの巡回群を表す。巡回群G_1, G_2の具体例は、楕円曲線Eのp等分点からなる有限集合E[p]やその部分群である。$G_1=G_2$であってもよいし$G_1\neq G_2$であってもよい。また、巡回群G_Tの具体例は、有限体F_qを基礎体とする拡大体を構成する有限集合である。その一例は、有限体F_qの代数閉包における１のｐ乗根からなる有限集合である。

[0019] なお、本形態では、巡回群G_1, G_2上で定義された演算を加法的に表現し、巡回群G_T上で定義された演算を乗法的に表現する。すなわち、$\chi\in F_q$及び$\Omega\in G_1$に対する$\chi\cdot\Omega\in G_1$は、$\Omega\in G_1$に対して巡回群G_1で定義された演算をχ回施すことを意味し、Ω_1, $\Omega_2\in G_1$に対する$\Omega_1+\Omega_2\in G_1$は、$\Omega_1\in G_1$と$\Omega_2\in G_1$とを被演算子として巡回群G_1で定義された演算を行うことを意味する。同様に、$\chi\in F_q$及び$\Omega\in G_2$に対する$\chi\cdot\Omega\in G_2$は、$\Omega\in G_2$に対して巡回群G_2で定義された演算をχ回施すことを意味し、Ω_1, $\Omega_2\in G_2$に対する$\Omega_1+\Omega_2\in G_2$は、$\Omega_1\in G_2$と$\Omega_2\in G_2$とを被演算子として巡回群G_2で定義された演算を行うことを意味する。一方、$\chi\in F_q$及び$\Omega\in G_T$に対する$\Omega^{\chi}\in G_T$は、$\Omega\in G_T$に対して巡回群G_Tで定義された

演算をχ回施すことを意味し、$\Omega_1, \Omega_2 \in G_T$に対する$\Omega_1 \cdot \Omega_2 \in G_T$は、$\Omega_1 \in G_T$と$\Omega_2 \in G_T$とを被演算子として巡回群$G_T$で定義された演算を行うことを意味する。

[0020] G_1^{n+1}：G_1^{n+1}はn+1(n≧1)個の巡回群G_1の直積を表す。

G_2^{n+1}：G_2^{n+1}はn+1個の巡回群G_2の直積を表す。

g_1, g_2, g_T：g_1, g_2, g_Tは巡回群G_1, G_2, G_Tの生成元を表す。

V：Vはn+1個の巡回群G_1の直積からなるn+1次元のベクトル空間を表す。

V*：V*はn+1個の巡回群G_2の直積からなるn+1次元のベクトル空間を表す。

[0021] e：eは直積G_1^{n+1}と直積G_2^{n+1}との直積$G_1^{n+1} \times G_2^{n+1}$を巡回群$G_T$に写す非退化な双線形写像（bilinear map）を計算するための関数（「双線形関数」と呼ぶ）を表す。双線形関数eは、巡回群G_1のn+1個の元γ_L(L=1,...,n+1)(n≧1)と巡回群G_2のn+1個の元γ_L^*(L=1,...,n+1)とを入力とし、巡回群G_Tの１個の元を出力する。

$$e : G_1^{n+1} \times G_2^{n+1} \rightarrow G_T \qquad \cdots(2)$$

[0022] 双線形関数eは以下の性質を満たす。

［双線形性］すべての$\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$及びν, $\kappa \in F_q$について以下の関係を満たす。

$$e(\nu \cdot \Gamma_1, \kappa \cdot \Gamma_2) = e(\Gamma_1, \Gamma_2)^{\nu \cdot \kappa} \qquad \cdots(3)$$

［非退化性］すべての

$$\Gamma_1 \in G_1^{n+1}, \quad \Gamma_2 \in G_2^{n+1} \qquad \cdots(4)$$

を巡回群G_Tの単位元に写す関数ではない。

［計算可能性］あらゆる$\Gamma_1 \in G_1^{n+1}$, $\Gamma_2 \in G_2^{n+1}$について$e(\Gamma_1, \Gamma_2)$を効率的に計算するアルゴリズムが存在する。

[0023] 本形態では、巡回群G_1と巡回群G_2との直積$G_1 \times G_2$を巡回群G_Tに写す非退化な双線形写像を計算するための関数

$$Pair : G_1 \times G_2 \rightarrow G_T \qquad \cdots(5)$$

を用いて双線形関数eを構成する。本形態の双線形関数eは、巡回群G_1のn+1個の元γ_L(L=1,...,n+1)からなるn+1次元ベクトル$(\gamma_1, \ldots, \gamma_{n+1})$と、巡回群$G_2$のn+1個の元$\gamma_L^*$(i=1,...,n+1)からなるn+1次元ベクトル$(\gamma_1^*, \ldots, \gamma_{n+1}^*)$との入

力に対し、巡回群G_Tの１個の元

$$e=\Pi_{L=1}^{n+1} \mathrm{Pair}(\gamma_L, \gamma_L^*) \quad \cdots(6)$$

を出力する関数である。

[0024] なお、双線形関数Pairは、巡回群G_1の１個の元と巡回群G_2の１個の元との組を入力とし、巡回群G_Tの１個の元を出力する関数であり、以下の性質を満たす。

［双線形性］すべての$\Omega_1 \in G_1$, $\Omega_2 \in G_2$及びν, $\kappa \in F_q$について以下の関係を満たす。

$$\mathrm{Pair}(\nu \cdot \Omega_1, \kappa \cdot \Omega_2)=\mathrm{Pair}(\Omega_1, \Omega_2)^{\nu \cdot \kappa} \quad \cdots(7)$$

［非退化性］すべての

$$\Omega_1 \in G_1, \ \Omega_2 \in G_2 \quad \cdots(8)$$

を巡回群G_Tの単位元に写す関数ではない。

［計算可能性］あらゆる$\Omega_1 \in G_1$, $\Omega_2 \in G_2$についてPair(Ω_1, Ω_2)を効率的に計算するアルゴリズムが存在する。

[0025] なお、双線形関数Pairの具体例は、Weilペアリングや Tateペアリングなどのペアリング演算を行うための関数である（例えば、参考文献４「Alfred. J. Menezes, ELLIPTIC CURVE PUBLIC KEY CRYPTOSYSTEMS, KLUWER ACADEMIC PUBLISHERS, ISBNO-7923-9368-6, pp. 61-81」等参照）。また、楕円曲線Eの種類に応じ、Tateペアリングなどのペアリング演算を行うための関数と所定の関数phiを組み合わせた変更ペアリング関数e(Ω_1,phi(Ω_2))（$\Omega_1 \in G_1$, $\Omega_2 \in G_2$）を双線形関数Pairとして用いてもよい（例えば、参考文献２等参照）。また、ペアリング演算をコンピュータ上で行うためのアルゴリズムとしては、周知のMiller のアルゴリズム（参考文献５「V. S. Miller, “Short Programs for functions on Curves,” 1986, インターネット<http://crypto.stanford.edu/miller/miller.pdf>」などが存在する。また、ペアリング演算を効率的に行うための楕円曲線や巡回群の構成方法はよく知られている（例えば、参考文献２、参考文献６「A. Miyaji, M. Nakabayashi, S.Takano, "New explicit conditions of elliptic curve Traces for FR-Reduction," IE

ICE Trans. Fundamentals, vol. E84-A, no05, pp. 1234-1243, May 2001」、参考文献７「P.S.L.M. Barreto, B. Lynn, M. Scott, "Constructing elliptic curves with prescribed embedding degrees," Proc. SCN '2002, LNCS 2576, pp.257-267, Springer-Verlag. 2003」、参考文献８「R. Dupont, A. Enge, F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields," http://eprint.iacr.org/2002/094/」等参照）。

[0026] a_i(i=1,...,n+1)：巡回群G_1のn+1個の元を要素とするn+1次元の基底ベクトルを表す。基底ベクトルa_iの一例は、$\kappa_1 \cdot g_1 \in G_1$をi次元目の要素とし、残りのn個の要素を巡回群$G_1$の単位元（加法的に「0」と表現）とするn+1次元の基底ベクトルである。この場合、n+1次元の基底ベクトルa_i(i=1,...,n+1)の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$a_1=(\kappa_1 \cdot g_1, 0, 0, \ldots, 0)$$
$$a_2=(0, \kappa_1 \cdot g_1, 0, \ldots, 0) \quad \cdots(9)$$
$$\ldots$$
$$a_{n+1}=(0, 0, 0, \ldots, \kappa_1 \cdot g_1)$$

[0027] ここで、κ_1は加法単位元0_F以外の有限体F_qの元からなる定数であり、$\kappa_1 \in F_q$の具体例は$\kappa_1=1_F$である。基底ベクトルa_iは直交基底であり、巡回群G_1のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルa_i(i=1,...,n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルa_iは前述のベクトル空間Vを張る。

[0028] a_i^*(i=1,...,n+1)：a_i^*は巡回群G_2のn+1個の元を要素とするn+1次元の基底ベクトルを表す。基底ベクトルa_i^*の一例は、$\kappa_2 \cdot g_2 \in G_2$をi次元目の要素とし、残りのn個の要素を巡回群$G_2$の単位元（加法的に「0」と表現）とするn+1次元の基底ベクトルである。この場合、基底ベクトルa_i^*(i=1,...,n+1)の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$a_1^*=(\kappa_2 \cdot g_2, 0, 0, \ldots, 0)$$
$$a_2^*=(0, \kappa_2 \cdot g_2, 0, \ldots, 0) \quad \cdots(10)$$
$$\ldots$$

$$a_{n+1}^{*}=(0,0,0,\ldots,\kappa_2\cdot g_2)$$

[0029] ここで、κ_2は加法単位元0_F以外の有限体F_qの元からなる定数であり、$\kappa_2\in F_q$の具体例は$\kappa_2=1_F$である。基底ベクトルa_i^{*}は直交基底であり、巡回群G_2のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルa_i^{*}(i=1,...,n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルa_i^{*}は前述のベクトル空間V^{*}を張る。

[0030] なお、基底ベクトルa_iと基底ベクトルa_i^{*}とは、0_Fを除く有限体F_qの元$\tau=\kappa_1\cdot\kappa_2$について

$$e(a_i,\ a_j^{*})=g_T^{\tau\cdot\delta(i,j)} \qquad \cdots(11)$$

を満たす。すなわち、i=jの場合には、式(6)(7)の関係から、

$$\begin{aligned} e(a_i,\ a_j^{*}) &= Pair(\kappa_1\cdot g_1,\kappa_2\cdot g_2)\cdot Pair(0,\ 0)\cdot\ldots\cdot Pair(0,\ 0)\\ &= Pair(g_1,\ g_2)^{\kappa1\cdot\kappa2}\cdot Pair(g_1,\ g_2)^{0\cdot0}\cdot\ldots\cdot Pair(g_1,\ g_2)^{0\cdot0}\\ &= Pair(g_1,\ g_2)^{\kappa1\cdot\kappa2}=g_T^{\tau}\end{aligned}$$

を満たす。一方、i≠jの場合には、$e(a_i,\ a_j^{*})$は、$Pair(\kappa_1\cdot g_1,\kappa_2\cdot g_2)$を含まず、$Pair(\kappa_1\cdot g_1,0)$と $Pair(0,\kappa_2\cdot g_2)$と$Pair(0,0)$との積になる。さらに、式(7)の関係から$Pair(g_1,\ 0)=Pair(0,\ g_2)=Pair(g_1,\ g_2)^0$を満たす。そのため、i≠jの場合には、

$$e(a_i,\ a_j^{*})=e(g_1,\ g_2)^0=g_T^0$$

を満たす。

[0031] 特に、$\tau=\kappa_1\cdot\kappa_2=1_F$である場合（例えば、$\kappa_1=\kappa_2=1_F$の場合）、

$$e(a_i,\ a_j^{*})=g_T^{\delta(i,j)} \qquad \cdots(12)$$

を満たす。ここで、$g_T^0=1$は巡回群G_Tの単位元であり、$g_T^1=g_T$は巡回群G_Tの生成元である。この場合、基底ベクトルa_iと基底ベクトルa_i^{*}とは双対正規直交基底であり、ベクトル空間Vとベクトル空間V^{*}とは、双線形写像を構成可能な双対ベクトル空間〔双対ペアリングベクトル空間（DPVS:Dual Paring Vector space)〕である。

[0032] A：Aは基底ベクトルa_i(i=1,...,n+1)を要素とするn+1行n+1列の行列を表す。例えば、基底ベクトルa_i(i=1,...,n+1)が式(9)によって表現される場合、行

列Aは、

[0033] [数1]

$$A=\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n+1} \end{pmatrix}=\begin{pmatrix} \kappa_1\cdot g_1 & 0 & \cdots & 0 \\ 0 & \kappa_1\cdot g_1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_1\cdot g_1 \end{pmatrix} \quad \cdots(13)$$

[0034] となる。

A* : A*は基底ベクトルa_i^*(i=1, . . . , n+1)を要素とするn+1行n+1列の行列を表す。例えば、基底ベクトルa_i^*(i=1, . . . , n+1)が式(10)によって表現される場合、行列A*は、

[0035] [数2]

$$A^*=\begin{pmatrix} a_1^* \\ a_2^* \\ \vdots \\ a_{n+1}^* \end{pmatrix}=\begin{pmatrix} \kappa_2\cdot g_2 & 0 & \cdots & 0 \\ 0 & \kappa_2\cdot g_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa_2\cdot g_2 \end{pmatrix} \quad \cdots(14)$$

[0036] となる。

X : Xは有限体F_qの元を要素とするn+1行n+1列の行列を表す。行列Xは基底ベクトルa_iの座標変換に用いられる。行列Xのi行j列(i=1, . . . , n+1, j=1, . . . , n+1)の要素を$\chi_{i,j}\in F_q$とすると、行列Xは、

[0037] [数3]

$$X=\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix} \quad \cdots(15)$$

[0038] となる。なお、行列Xの各要素$\chi_{i,j}$を変換係数と呼ぶ。

X* : X*は行列Xの逆行列の転置行列$X^*=(X^{-1})^T$を表す。行列X*は基底ベクトルa_i^*の座標変換に用いられる。行列X*のi行j列の要素を$\chi_{i,j}^*\in F_q$とすると、行列X*は、

[0039] [数4]

$$X^{*}=\begin{pmatrix} \chi_{1,1}^{*} & \chi_{1,2}^{*} & \cdots & \chi_{1,n+1}^{*} \\ \chi_{2,1}^{*} & \chi_{2,2}^{*} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1}^{*} & \chi_{n+1,2}^{*} & \cdots & \chi_{n+1,n+1}^{*} \end{pmatrix} \quad \cdots(16)$$

[0040] となる。なお、行列X*の各要素$\chi_{i,j}^{*}$を変換係数と呼ぶ。

この場合、n+1行n+1列の単位行列をIとすると$X\cdot(X^{*})^{T}=I$を満たす。すなわち、単位行列

[0041] [数5]

$$I=\begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix} \quad \cdots(17)$$

[0042] に対し、

[0043] [数6]

$$\begin{pmatrix} \chi_{1,1} & \chi_{1,2} & \cdots & \chi_{1,n+1} \\ \chi_{2,1} & \chi_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{n+1,1} & \chi_{n+1,2} & \cdots & \chi_{n+1,n+1} \end{pmatrix}\cdot\begin{pmatrix} \chi_{1,1}^{*} & \chi_{2,1}^{*} & \cdots & \chi_{n+1,1}^{*} \\ \chi_{1,2}^{*} & \chi_{2,2}^{*} & & \vdots \\ \vdots & & \ddots & \vdots \\ \chi_{1,n+1}^{*} & \chi_{2,n+1}^{*} & \cdots & \chi_{n+1,n+1}^{*} \end{pmatrix} \quad \cdots(18)$$

$$=\begin{pmatrix} 1_F & 0_F & \cdots & 0_F \\ 0_F & 1_F & & \vdots \\ \vdots & & \ddots & 0_F \\ 0_F & 0_F & \cdots & 1_F \end{pmatrix}$$

[0044] を満たす。ここで、n+1次元ベクトル

$$\chi_{i}^{\rightarrow}=(\chi_{i,1},\ldots,\chi_{i,n+1}) \quad \cdots(19)$$

$$\chi_{j}^{\rightarrow *}=(\chi_{j,1}^{*},\ldots,\chi_{j,n+1}^{*}) \quad \cdots(20)$$

を定義する。すると、式(18)の関係から、n+1次元ベクトル$\chi_{i}^{\rightarrow}$と$\chi_{j}^{\rightarrow *}$との内積は、

$$\chi_i^{\rightarrow} \cdot \chi_j^{\rightarrow *} = \delta(i, j) \qquad \cdots(21)$$

となる。

[0045] b_i : b_iは巡回群G_1のn+1個の元を要素とするn+1次元の基底ベクトルを表す。基底ベクトルb_iは行列Xを用いて基底ベクトルa_i (i=1, . . . , n+1)を座標変換することで得られる。具体的には、基底ベクトルb_iは、

$$b_i = \Sigma_{j=1}^{n+1} \chi_{i,j} \cdot a_j \qquad \cdots(22)$$

の演算によって得られる。例えば、基底ベクトルa_j (j=1, . . . , n+1)が式(9)によって表現される場合、基底ベクトルb_iの各要素をそれぞれ列挙して表現すると、以下のようになる。

$$b_i = (\chi_{i,1} \cdot \kappa_1 \cdot g_1 \ , \chi_{i,2} \cdot \kappa_1 \cdot g_1 \ , \ldots , \chi_{i,n+1} \cdot \kappa_1 \cdot g_1) \qquad \cdots(23)$$

[0046] 巡回群G_1のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルb_i (i=1, . . . , n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルb_iは前述のベクトル空間Vを張る。

[0047] b_i^* : b_i^*は巡回群G_2のn+1個の元を要素とするn+1次元の基底ベクトルを表す。行列X^*を用いて基底ベクトルa_i^*(i=1, . . . , n+1)を座標変換することで得られる。具体的には、基底ベクトルb_i^*は、

$$b_i^* = \Sigma_{j=1}^{n+1} \chi_{i,j}^* \cdot a_j^* \qquad \cdots(24)$$

の演算によって得られる。例えば、基底ベクトルa_j^*(j=1, . . . , n+1)が式(10)によって表現される場合、基底ベクトルb_i^*の各要素をそれぞれ列挙して表現すると、以下のようになる。

$$b_i^* = (\chi_{i,1}^* \cdot \kappa_2 \cdot g_2 \ , \chi_{i,2}^* \cdot \kappa_2 \cdot g_2 \ , \ldots , \chi_{i,n+1}^* \cdot \kappa_2 \cdot g_2) \qquad \cdots(25)$$

巡回群G_2のn+1個の元を要素とするすべてのn+1次元ベクトルは、n+1次元の基底ベクトルb_i^*(i=1, . . . , n+1)の線形和によって表される。すなわち、n+1次元の基底ベクトルb_i^*は前述のベクトル空間V^*を張る。

[0048] なお、基底ベクトルb_iと基底ベクトルb_i^*とは、0_Fを除く有限体F_qの元$\tau = \kappa_1 \cdot \kappa_2$について

$$e(b_i, \ b_j^*) = g_T^{\tau \cdot \delta(i,j)} \qquad \cdots(26)$$

を満たす。すなわち、式(6)(21)(23)(25)の関係から、

[0049] [数7]

$$
\begin{aligned}
e(b_i, b_j^*) &= \prod_{L=1}^{n+1} \mathrm{Pair}(\chi_{i,L} \cdot \kappa_1 \cdot g_1, \chi_{j,L}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathrm{Pair}(\chi_{i,1} \cdot \kappa_1 \cdot g_1, \chi_{j,1}^* \cdot \kappa_2 \cdot g_2) \cdot \ldots \cdot (\chi_{i,n} \cdot \kappa_1 \cdot g_1, \chi_{j,n}^* \cdot \kappa_2 \cdot g_2) \\
&\quad \times \mathrm{Pair}(\chi_{j,n+1} \cdot \kappa_1 \cdot g_1, \chi_{j,n+1}^* \cdot \kappa_2 \cdot g_2) \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,1} \cdot \chi_{j,1}^*} \cdot \ldots \cdot \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,2} \cdot \chi_{j,2}^*} \\
&\quad \times \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \chi_{i,n+1} \cdot \chi_{j,n+1}^*} \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 (\chi_{i,1} \cdot \chi_{j,1}^* + \chi_{i,2} \cdot \chi_{j,2}^* + \ldots + \chi_{i,n+1} \cdot \chi_{j,n+1}^*)} \\
&= \mathrm{Pair}(g_1, g_2)^{\kappa_1 \cdot \kappa_2 \cdot \vec{\chi_i} \cdot \vec{\chi_j}^*} \\
&= \mathrm{Pair}(g_1, g_2)^{\tau \cdot \delta(i,j)} = g_T^{\tau \cdot \delta(i,j)}
\end{aligned}
$$

[0050] を満たす。特に、$\tau = \kappa_1 \cdot \kappa_2 = 1_F$である場合（例えば、$\kappa_1 = \kappa_2 = 1_F$の場合）、

$$e(b_i, b_j^*) = g_T^{\delta(i,j)} \qquad \cdots (27)$$

を満たす。この場合、基底ベクトルb_iと基底ベクトルb_i^*とは、双対ペアリングベクトル空間（ベクトル空間Vとベクトル空間V*）の双対正規直交基底である。

なお、式(26)の関係を満たすのであれば、式(9)(10)で例示したもの以外の基底ベクトルa_i及びa_i^*や、式(22)(24)で例示したもの以外の基底ベクトルb_i及びb_i^*を用いてもよい。

[0051] B：Bは基底ベクトルb_i (i=1, . . . , n+1)を要素とするn+1行n+1列の行列を表す。B=X・Aを満たす。例えば、基底ベクトルb_iが式(23)によって表現される場合、行列Bは、

[0052]

[数8]

$$B=\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} \chi_{1,1}\cdot\kappa_1\cdot g_1 & \chi_{1,2}\cdot\kappa_1\cdot g_1 & \cdots & \chi_{1,n+1}\cdot\kappa_1\cdot g_1 \\ \chi_{2,1}\cdot\kappa_1\cdot g_1 & \chi_{2,2}\cdot\kappa_1\cdot g_1 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1}\cdot\kappa_1\cdot g_1 \\ \chi_{n+1,1}\cdot\kappa_1\cdot g_1 & \cdots & \chi_{n+1,n}\cdot\kappa_1\cdot g_1 & \chi_{n+1,n+1}\cdot\kappa_1\cdot g_1 \end{pmatrix} \quad \cdots(28)$$

[0053] となる。

B* : B*は基底ベクトルb_i^*(i=1, . . . , n+1)を要素とするn+1行n+1列の行列を表す。B*=X*・A*を満たす。例えば、基底ベクトルb_i^*(i=1, . . . , n+1)が式(25)によって表現される場合、行列B*は、

[0054] [数9]

$$B^*=\begin{pmatrix} b_1^* \\ b_2^* \\ \vdots \\ b_{n+1}^* \end{pmatrix} = \begin{pmatrix} \chi_{1,1}^*\cdot\kappa_2\cdot g_2 & \chi_{1,2}^*\cdot\kappa_2\cdot g_2 & \cdots & \chi_{1,n+1}^*\cdot\kappa_2\cdot g_2 \\ \chi_{2,1}^*\cdot\kappa_2\cdot g_2 & \chi_{2,2}^*\cdot\kappa_2\cdot g_2 & & \vdots \\ \vdots & & \ddots & \chi_{n,n+1}^*\cdot\kappa_2\cdot g_2 \\ \chi_{n+1,1}^*\cdot\kappa_2\cdot g_2 & \cdots & \chi_{n+1,n}^*\cdot\kappa_2\cdot g_2 & \chi_{n+1,n+1}^*\cdot\kappa_2\cdot g_2 \end{pmatrix} \quad \cdots(29)$$

[0055] となる。

$\vec{w}$: $\vec{w}$は有限体F_qの元を要素とするn次元ベクトルを表す。

$$\vec{w}=(w_1,\ldots,w_n)\in F_q^n \quad \cdots(30)$$

w_μ : w_μはn次元ベクトルのμ(μ=1, . . . , n)番目の要素を表す。

$\vec{v}$: $\vec{v}$は有限体F_qの元を要素とするn次元ベクトルを表す。

$$\vec{v}=(v_1,\ldots,v_n)\in F_q^n \quad \cdots(31)$$

v_μ : v_μはn次元ベクトルのμ(μ=1, . . . , n)番目の要素を表す。

[0056] 衝突困難な関数：「衝突困難な関数」とは、十分大きなセキュリティパラメータkに対して以下の条件を満たす関数h、又は、それとみなせる関数を表す。

$$Pr[A(h)=(x,y)|h(x)=h(y)\wedge x\neq y]<\varepsilon(k) \quad \cdots(32)$$

ただし、Pr[・]は事象[・]の確率であり、A(h)は関数hに対してh(x)=h(y)を満たす値x,y（x≠y）を算出する確率的多項式時間アルゴリズムであり、ε(k)はセキュリティパラメータkについての多項式である。衝突困難な関数の例は、参考文献１に開示された「cryptographic hash function」などのハッシュ関数である。

[0057] 単射関数：「単射関数」とは、値域に属する元が何れもその定義域のただ一つの元の像として表される関数、又は、それとみなせる関数を表す。

[0058] 擬似的なランダム関数：「擬似的なランダム関数」とは、任意の確率的多項式時間アルゴリズムが集合Φ_ζとその部分集合ϕ_ζとを区別できない場合における、当該部分集合ϕ_ζに属する関数、又は、それとみなせる関数を表す。ただし、集合Φ_ζは集合$\{0,1\}^\zeta$の元を集合$\{0,1\}^\zeta$の元へ写すすべての関数の集合である。擬似的なランダム関数の例は、上述のようなハッシュ関数である。

[0059] H_1：H_1は２つのバイナリ系列（ω_1,ω_2）$\in\{0,1\}^k\times\{0,1\}^*$を入力とし、有限体$F_q$の２つの元（$\psi_1,\psi_2$）$\in F_q\times F_q$を出力する衝突困難な関数を表す。

$$H_1:\{0,1\}^k\times\{0,1\}^*\rightarrow F_q\times F_q \quad \cdots(33)$$

[0060] このような関数H_1の例は、ω_1とω_2とのビット連結値$\omega_1||\omega_2$を入力とし、参考文献１に開示された「cryptographic hash function」などのハッシュ関数と、「バイナリ系列から整数への変換関数（Octet string/integer conversion）」と、「バイナリ系列から有限体の元への変換関数（Octet string and integer/finite field conversion）」との演算を行い、有限体F_qの２つの元（ψ_1,ψ_2）$\in F_q\times F_q$を出力する関数である。なお、関数H_1は、擬似的なランダム関数であることが望ましい。

[0061] H_2：H_2は巡回群G_Tの元とバイナリ系列（ξ,ω_2）$\in G_T\times\{0,1\}^*$を入力とし、有

限体F_qの１つの元$\psi \in F_q$を出力する衝突困難な関数を表す。

$$H_2 : G_T \times \{0,1\}^* \rightarrow F_q \quad \cdots(34)$$

[0062] このような関数H_2の例は、巡回群G_Tの元$\xi \in G_T$とバイナリ系列$\omega_2 \in \{0,1\}^*$とを入力とし、巡回群G_Tの元$\xi \in G_T$を参考文献１に開示された「有限体の元からバイナリ系列への変換関数（Octet string and integer/finite field conversion）」に入力してバイナリ系列を求め、そのバイナリ系列とバイナリ系列$\omega_2 \in \{0,1\}^*$とのビット連結値に対して参考文献１に開示された「cryptographic hash function」などのハッシュ関数演算を行い、さらに「バイナリ系列から有限体の元への変換関数（Octet string and integer/finite field conversion）」の演算を行い、有限体F_qの１つの元$\psi \in F_q$を出力する関数である。なお、安全性の観点から、関数H_2は擬似的なランダム関数であることがより望ましい。

[0063] R:Rは１つの巡回群G_Tの元$\xi \in G_T$を入力とし、１つのバイナリ系列$\omega \in \{0,1\}^k$を出力する単射関数を表す。

$$R : G_T \rightarrow \{0,1\}^k \quad \cdots(35)$$

[0064] このような単射関数Rの例は、巡回群G_Tの元$\xi \in G_T$を入力とし、参考文献１に開示された「有限体の元からバイナリ系列への変換関数（Octet string and integer/finite field conversion）」と、参考文献１に開示された「KDF(Key Derivation Function)」などのハッシュ関数との演算を行い、１つのバイナリ系列$\omega \in \{0,1\}^k$を出力する関数である。なお、安全性の観点から、関数Rは衝突困難な関数であることが望ましく、擬似的なランダム関数であることがより望ましい。

[0065] Enc：Encは共通鍵暗号方式の暗号化処理を示す共通鍵暗号関数を表す。共通鍵暗号方式の具体例は、カメリア（Camellia）やAESなどである。

$Enc_k(M)$：$Enc_k(M)$は、共通鍵Kを用い、共通鍵暗号関数Encに従って平文Mを暗号化して得られた暗号文を表す。

Dec：Decは、共通鍵暗号方式の復号処理を示す共通鍵復号関数を表す。

$Dec_k(C)$：$Dec_k(C)$は、共通鍵Kを用い、共通鍵復号関数Decに従って暗号文C

を復号して得られた復号結果を表す。

[0066] 〔内積述語暗号〕

次に、内積述語暗号の基本的な構成について説明する。

＜述語暗号＞

述語暗号（「関数暗号」と呼ぶ場合もある）とは、「属性情報」と呼ばれる情報と「述語情報」と呼ばれる情報との組み合わせが所定の論理式を「真」にする場合に暗号文が復号できる方式である。「属性情報」と「述語情報」の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。従来の述語暗号の構成は、例えば、参考文献９「"Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products," with Amit Sahai and Brent Waters One of 4 papers from Eurocrypt 2008 invited to the Journal of Cryptology」等に開示されている。

[0067] ＜内積述語暗号＞

内積述語暗号は、属性情報や述語情報としてベクトルを用い、それらの内積が０となる場合に暗号文が復号される述語暗号である。内積述語暗号では、内積が０となることと論理式が「真」となることとが等価である。

[0068] ［論理式と多項式との関係］

内積述語暗号では、論理和や論理積からなる論理式を多項式で表現する。

まず、「xがη_1である」という命題１と「xがη_2である」という命題２との論理和 $(x=\eta_1)\vee(x=\eta_2)$ を

$$(x-\eta_1)\cdot(x-\eta_2) \qquad \cdots(36)$$

という多項式で表現する。すると、各真理値と式(36)の関数値との関係は以下のようになる。

[0069] ［表1］

命題１ $(x=\eta_1)$	命題２ $(x=\eta_2)$	論理和 $(x=\eta_1)\vee(x=\eta_2)$	関数値 $(x-\eta_1)\cdot(x-\eta_2)$
真	真	真	0
真	偽	真	0
偽	真	真	0
偽	偽	偽	その他

[表1]から分かるように、論理和$(x=\eta_1)\vee(x=\eta_2)$が真である場合、式(36)の関数値は0になり、論理和$(x=\eta_1)\vee(x=\eta_2)$が偽である場合、式(36)の関数値は0以外の値となる。すなわち、論理和$(x=\eta_1)\vee(x=\eta_2)$が真であることと、式(36)の関数値が0となることとは等価である。よって、論理和は式(36)で表現できる。

[0070] また、「xがη_1である」という命題１と「xがη_2である」という命題２との論理積 $(x=\eta_1)\wedge(x=\eta_2)$を

$$\iota_1\cdot(x-\eta_1)+\iota_2\cdot(x-\eta_2) \qquad \cdots(37)$$

という多項式で表現する。ただし、ι_1及びι_2は乱数である。すると、真理値と式(37)の関数値とは以下の関係となる。

[0071] [表2]

命題１ $(x=\eta_1)$	命題２ $(x=\eta_2)$	論理積 $(x=\eta_1)\wedge(x=\eta_2)$	関数値 $\iota_1\cdot(x-\eta_1)+\iota_2\cdot(x-\eta_2)$
真	真	真	0
真	偽	偽	その他
偽	真	偽	その他
偽	偽	偽	その他

[表２]から分かるように、論理積 $(x=\eta_1)\wedge(x=\eta_2)$が真である場合、式(37)の関数値は0になり、論理積 $(x=\eta_1)\wedge(x=\eta_2)$が偽である場合、式(37)の関数値は0以外の値となる。すなわち、論理積 $(x=\eta_1)\wedge(x=\eta_2)$が真であることと、式(37)の関数値が0となることとは等価である。よって、論理積は式(37)で表現できる。

[0072] 以上のように、式(36)と式(37)とを用いることで論理和や論理積からなる論理式を多項式f(x)で表現できる。例えば、論理式$\{(x=\eta_1)\vee(x=\eta_2)\vee(x=\eta_3)\}\wedge(x=\eta_4)\wedge(x=\eta_5)$は、多項式

$$f(x)=\iota_1\cdot\{(x-\eta_1)\cdot(x-\eta_2)\cdot(x-\eta_3)\}+\iota_2\cdot(x=\eta_4)+\iota_3\cdot(x=\eta_5) \quad \cdots(38)$$

で表現できる。

[0073] なお、式(36) では、１つの不定元xを用いて論理和を表現したが、複数の不定元を用いて論理和を表現することも可能である。例えば、２つの不定元x_0

及びx_1を用い、「x_0がη_0である」という命題１と「x_1がη_1である」という命題２との論理和 $(x_0=\eta_0)\vee(x_1=\eta_1)$を

$$(x_0-\eta_0)\cdot(x_1-\eta_1)$$

という多項式で表現することも可能であり、３つ以上の不定元を用い、論理和を多項式で表現することも可能である。

[0074] また、式(37)では、１つの不定元xを用いて論理積を表現したが、複数の不定元を用いて論理積を表現することも可能である。例えば、また、「x_0がη_0である」という命題１と「x_1がη_1である」という命題２との論理積 $(x_0=\eta_0)\wedge(x_1=\eta_1)$を

$$\iota_0\cdot(x_0-\eta_0)+\iota_1\cdot(x_1-\eta_1)$$

という多項式で表現することも可能であり、３つ以上の不定元を用い、論理積を多項式で表現することも可能である。

[0075] 論理和及び／又は論理積を含む論理式をH(H≧1)種類の不定元$x_0,\ldots,x_{H-1}$を用いて表現した多項式を$f(x_0,\ldots,x_{H-1})$と表現する。また、各不定元$x_0,\ldots,x_{H-1}$に対応する命題を「x_hがη_hである」とする。ただし、η_h (h=0,...H-1) は命題ごとに定まる定数である。この場合、当該論理式を示す多項式$f(x_0,\ldots,x_{H-1})$は、不定元x_hと定数η_hとの差をとる多項式によって当該不定元x_hが当該定数η_hであるという命題を表現し、命題をそれぞれ表現する多項式の積によって当該命題の論理和を表現し、命題又は命題の論理和をそれぞれ表現する多項式の線形和によって当該命題又は命題の論理和の論理積を表現し、それによって論理式を表現した多項式となる。例えば、５つの不定元$x_0,\ldots,x_4$を用い、論理式$\{(x_0=\eta_0)\vee(x_1=\eta_1)\vee(x_2=\eta_2)\}\wedge(x_3=\eta_3)\wedge(x_4=\eta_4)$を多項式で表現すると、

$$f(x_0,\ldots,x_4)$$
$$=\iota_0\cdot\{(x_0-\eta_0)\cdot(x_1-\eta_1)\cdot(x_2-\eta_2)\}+\iota_1\cdot(x_3=\eta_3)+\iota_2\cdot(x_4=\eta_4)$$

となる。

[0076] ［多項式と内積の関係］

論理式を示す多項式$f(x_0,\ldots,x_{H-1})$は、２つのn次元ベクトルの内積で表現で

きる。すなわち、多項式$f(x_0,\ldots,x_{H-1})$は、当該多項式$f(x_0,\ldots,x_{H-1})$の各項の不定元成分を各要素とするベクトル

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

と、当該多項式$f(x_0,\ldots,x_{H-1})$の各項の係数成分を各要素とするベクトル

$$\vec{w}=(w_1,\ldots,w_n)$$

との内積

$$f(x_0,\ldots,x_{H-1})=\vec{w}\cdot\vec{v}$$

に等しい。すなわち、論理式を示す多項式$f(x_0,\ldots,x_{H-1})$が0であるか否かと、多項式$f(x_0,\ldots,x_{H-1})$の各項の不定元成分を各要素とするベクトル$\vec{v}$と、多項式$f(x_0,\ldots,x_{H-1})$の各項の係数成分を各要素とするベクトル$\vec{w}$との内積が0であるか否かとは等価である。

[0077] $$f(x_0,\ldots,x_{H-1})=0 \quad\longleftrightarrow\quad \vec{w}\cdot\vec{v}=0$$

例えば、１つの不定元xで表現された多項式$f(x)=\theta_0\cdot x^0+\theta_1\cdot x+\ldots+\theta_{n-1}\cdot x^{n-1}$は、２つのn次元ベクトル

$$\vec{w}=(w_1,\ldots,w_n)=(\theta_0,\ldots,\theta_{n-1}) \qquad \cdots(39)$$

$$\vec{v}=(v_1,\ldots,v_n)=(x^0,\ldots,x^{n-1}) \qquad \cdots(40)$$

の内積

$$f(x)=\vec{w}\cdot\vec{v} \qquad \cdots(41)$$

で表現できる。すなわち、論理式を示す多項式$f(x)$が0であるか否かと、式(41)の内積が0であるか否かとは等価である。

[0078] $$f(x)=0 \quad\longleftrightarrow\quad \vec{w}\cdot\vec{v}=0 \qquad \cdots(42)$$

また、多項式$f(x_0,\ldots,x_{H-1})$の各項の不定元成分を各要素とするベクトルを

$$\vec{w}=(w_1,\ldots,w_n)$$

とし、多項式$f(x_0,\ldots,x_{H-1})$の各項の係数成分を各要素とするベクトル

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

としても、論理式を示す多項式$f(x_0,\ldots,x_{H-1})$が0であるか否かと、ベクトル$\vec{w}$とベクトル$\vec{v}$との内積が0であるか否かとは等価である。

[0079] 例えば、式(39)(40)の代わりに

$$\vec{w}=(w_{1,\ldots,}w_n)=(x^{0}_{,\ldots,}x^{n}) \quad \cdots(43)$$

$$\vec{v}=(v_{1,\ldots,}v_n)=(\theta_{1,\ldots,}\theta_{n-1}) \quad \cdots(44)$$

としても、論理式を示す多項式f(x)が0であるか否かと、式(41)の内積が0であるか否かとは等価である。

[0080] 内積述語暗号では、ベクトル$\vec{v}=(v_{0,\ldots,}v_{n-1})$及び$\vec{w}=(w_{0,\ldots,}w_{n-1})$の何れか一方を属性情報とし、他方を述語情報とし、属性情報と述語情報の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。例えば、n次元ベクトル$(\theta_{0,\ldots,}\theta_{n-1})$が述語情報とされ、n次元ベクトル$(x^{0}_{,\ldots,}x^{n-1})$が属性情報とされ、属性情報と述語情報の一方が暗号文に埋め込まれ、他方が鍵情報に埋め込まれる。なお、以下では、鍵情報に埋め込まれるn次元ベクトルを$\vec{w}=(w_{1,\ldots,}w_n)$とし、暗号文に埋め込まれるn次元ベクトルを$\vec{v}=(v_{1,\ldots,}v_n)$とする。例えば、

述語情報：$\vec{w}=(w_{1,\ldots,}w_n)=(\theta_{0,\ldots,}\theta_{n-1})$

属性情報：$\vec{v}=(v_{1,\ldots,}v_n)=(x^{0}_{,\ldots,}x^{n-1})$

であるか、

述語情報：$\vec{v}=(v_{1,\ldots,}v_n)=(\theta_{0,\ldots,}\theta_{n-1})$

属性情報：$\vec{w}=(w_{1,\ldots,}w_n)=(x^{0}_{,\ldots,}x^{n-1})$

である。

[0081] [内積述語暗号の基本構成]

以下では、内積述語暗号を用いて鍵カプセル化メカニズムKEM (Key Encapsulation Mechanisms)を構成する場合の基本構成を例示する。この構成はSetup(1^k), GenKey(MSK,$\vec{w}$), Enc(PA,$\vec{v}$), Dec(SKw,C_2)を含む。

[0082] 《Setup(1^k)：セットアップ》

－入力：セキュリティパラメータk

－出力：マスター鍵情報MSK, 公開パラメータPK

Setup(1^k)の一例では、まず、セキュリティパラメータkをnとして、n+1次元の基底ベクトルa_i(i=1,...,n+1)を要素とするn+1行n+1列の行列Aと、基底ベクトルa_i^*(i=1,...,n+1)を要素とするn+1行n+1列の行列A*と、座標変換のためのn+1行n+1列の行列X, X*とが選択される。次に、式(22)に従って座標変換された

n+1次元の基底ベクトルb_i(i=1,...,n+1)が算出され、式(24)に従って座標変換されたn+1次元の基底ベクトルb_i^*(i=1,...,n+1)が算出される。そして、基底ベクトルb_i^*(i=1,...,n+1)を要素とするn+1行n+1列の行列B*がマスター鍵情報MSKとして出力され、ベクトル空間V, V*、基底ベクトルb_i(i=1,...,n+1)を要素とするn+1行n+1列の行列B、セキュリティパラメータk、有限体F_q、楕円曲線E、巡回群G_1, G_2, G_T、生成元g_1, g_2, g_T、双線形関数eなどが公開パラメータPKとして出力される。

[0083] 《GenKey(MSK,$\vec{w}$):鍵情報生成》

ー入力:マスター鍵情報MSK, ベクトル$\vec{w}$

ー出力:ベクトル$\vec{w}$に対応する鍵情報D*

GenKey(MSK,$\vec{w}$)の一例では、まず、有限体F_qから元$\alpha \in F_q$が選択される。そして、マスター鍵情報MSKである行列B*を用い、ベクトル$\vec{w}$に対応する鍵情報

$$D^* = \alpha \cdot (\Sigma_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^* \in G_2^{n+1} \quad \cdots(45)$$

が生成され、出力される。なお、巡回群G_2上での離散対数問題の求解が困難である場合、鍵情報D*から$w_\mu \cdot b_\mu^*$やb_{n+1}^*の成分を分離抽出することは困難である。

[0084] 《Enc(PA,$\vec{v}$):暗号化》

ー入力:公開パラメータPK, ベクトル$\vec{v}$

ー出力:暗号文C_2, 共通鍵K

Enc(PA,$\vec{v}$)の一例では、まず、共通鍵Kと有限体F_qの元である乱数υ_1とが生成される。そして、行列Bなどの公開パラメータPKと、共通鍵Kを含む値に対応する有限体F_qの元υ_2と、ベクトル$\vec{v}$と、乱数υ_1とを用い、暗号文

$$C_2 = \upsilon_1 \cdot (\Sigma_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1} \in G_1^{n+1} \quad \cdots(46)$$

が生成される。そして、暗号文C_2と共通鍵Kとが出力される。共通鍵Kの一例は$K = g_T^{\tau \cdot \upsilon 2} \in G_T$である。ここで、添え字の$\upsilon 2$は$\upsilon_2$を意味する。また、前述のように$\tau$の一例は$\tau = 1_F$である。なお、巡回群$G_1$上での離散対数問題の求解が困難である場合、暗号文$C_2$から$v_\mu \cdot b_\mu$や$\upsilon_2 \cdot b_{n+1}$の成分を分離抽出することは困難である。

[0085] 《Dec(SKw, C_2) : 復号・鍵共有》

ー入力：ベクトルw→に対応する鍵情報D_1^*, 暗号文C_2

ー出力：共通鍵K

Dec(SKw, C_2)の一例では、まず、暗号文C_2と鍵情報D_1^*とが式(2)の双線形関数eに入力される。すると、式(3)(26)の性質から、

[0086] [数10]

$$\begin{aligned} e(C_2, D^*) &= e(\upsilon_1 \cdot (\sum_{\mu=1}^{n} v_\mu \cdot b_\mu) + \upsilon_2 \cdot b_{n+1}, \alpha \cdot (\sum_{\mu=1}^{n} w_\mu \cdot b_\mu^*) + b_{n+1}^*) \\ &= e(\upsilon_1 \cdot v_1 \cdot b_1, \alpha \cdot w_1 \cdot b_1^*) \cdot \ldots \cdot e(\upsilon_1 \cdot v_n \cdot b_n, \alpha \cdot w_n \cdot b_n^*) \\ &\quad \times e(\upsilon_2 \cdot b_{n+1}, b_{n+1}^*) \\ &= e(b_1, b_1^*)^{\upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot e(b_n, b_n^*)^{\upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot e(b_{n+1}, b_{n+1}^*)^{\upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot v_1 \cdot \alpha \cdot w_1} \cdot \ldots \cdot g_T^{\tau \cdot \upsilon_1 \cdot v_n \cdot \alpha \cdot w_n} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot v^\rightarrow \cdot w^\rightarrow} \cdot g_T^{\tau \cdot \upsilon_2} \end{aligned} \quad \cdots (47)$$

[0087] を満たす。

ここで、内積w→・v→=0であれば、式(47)は、

[0088] [数11]

$$\begin{aligned} e(C_2, D^*) &= g_T^{\tau \cdot \upsilon_1 \cdot \alpha \cdot 0} \cdot g_T^{\tau \cdot \upsilon_2} \\ &= g_T^{\tau \cdot \upsilon_2} \end{aligned} \quad \cdots (48)$$

[0089] と変形できる。この結果から共通鍵Kが生成され出力される。共通鍵Kの一例は$K=g_T^{\tau \cdot \upsilon 2} \in G_T$である。

[0090] [第一実施形態]

第一実施形態の情報生成装置及び方法は、前述した述語暗号を用いて階層型暗号を実現したものである。具体的には、前述した述語暗号で登場する基底ｂ*を用いて、木構造以外の一般の半順序構造で表される情報導出を実現するものである。

図１に、第一実施形態の情報生成装置の機能ブロック図を例示する。

[0091] 各情報には、インデックスｖが付けられている。インデックスｖは、ｖ＝（v_1, …, v_{N-1}）∈Ｉ＝（F_q∪｛＊｝）$^{N-1}$であり、インデックスｖには

対応する集合ｗ（ｖ）＝｛ｉ｜ｖ$_{i}$＝＊｝が定義されている。＊は不定文字である。以下に登場するインデックスｕ，インデックスＹ等のインデックスはインデックスｖと同様の構造を持ち、インデックスｕ＝（ｕ$_{1}$，…，ｕ$_{N-1}$）∈Ｉ＝（Ｆ$_{q}$Ｕ｛＊｝）$^{N-1}$、インデックスＹ＝（Ｙ$_{1}$，…，Ｙ$_{N-1}$）∈Ｉ＝（Ｆ$_{q}$Ｕ｛＊｝）$^{N-1}$であるとする。インデックスｕ∈Ｉとインデックスｖ∈Ｉに対して、ｗ（ｕ）⊂ｗ（ｖ）かつｖ$_{i}$＝ｕ$_{i}$（ｉ∈｛１，…，Ｎ－１｝＼ｗ（ｖ））であるとき、すなわち、ｗ（ｕ）⊂ｗ（ｖ）かつ任意のｉ∈｛１，…，Ｎ－１｝＼ｗ（ｖ）に対してｖ$_{i}$＝ｕ$_{i}$であるとき、インデックスｕ≦インデックスｖであり、インデックスｖはインデックスｕよりも上位の情報であるとする。ここで、記号「＼」は集合の減算を意味し、例えば集合Ａ＝｛１，２，３｝、集合Ｂ＝｛１｝のとき、Ａ＼Ｂ＝｛２，３｝である。

[0092] 例えば、インデックスｖ＝｛ｖ$_{1}$，ｖ$_{2}$，ｖ$_{3}$｝＝｛２，＊，＊｝であり、インデックスｕ＝｛ｕ$_{1}$，ｕ$_{2}$，ｕ$_{3}$｝＝｛２，＊，４｝であるとする。このとき、ｗ（ｖ）＝｛２，３｝、ｗ（ｕ）＝｛２｝となり、ｗ（ｕ）⊂ｗ（ｖ）が成立する。また、ｖ$_{1}$＝ｕ$_{1}$＝２である。したがって、インデックスｕ≦インデックスｖであり、インデックスｖはインデックスｕよりも上位の情報であるといえる。

[0093] 以下、基底ｂ$_{i}$＊から生成される情報に対するインデックスをインデックスＹと表記し、導出基の情報に対するインデックスをインデックスｖと表記し、その導出基の情報から導出された情報に対するインデックスをインデックスｕと表記する。

[0094] ＜情報生成＞

情報生成装置及び方法は、図２のステップＡ１からステップＡ３において、基底ｂ$_{i}$＊を用いてインデックスＹに対応する情報Ｋ$_{Y}$を生成する。情報Ｋ$_{Y}$は、主情報ｋ$_{Y}$と導出情報ｋ$_{Yj}$とを含む。主情報ｋ$_{Y}$は、述語暗号において例えば復号鍵として使用される。導出情報ｋ$_{Yj}$は、インデックスＹに対応する情報Ｋ$_{Y}$よりも下位の情報を生成するために用いられる。

[0095] 情報生成装置には、インデックスＹ∈Ｉが入力される。

乱数生成部１は、乱数$\sigma_Y \in Z_q$、及び、集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）に対応する乱数$\sigma_{Yj} \in Z_q$を生成する（ステップＡ１）。生成された乱数σ_Yは、主情報生成部２に送られる。生成された乱数σ_{Yj}は、導出情報生成部３に送られる。例えば、集合ｗ（Ｙ）＝｛２，３｝である場合には、乱数生成部１はσ_Y、σ_{Y2}及びσ_{Y3}の３つの乱数を生成する。

[0096] 主情報生成部２は、上記生成された乱数σ_Yを用いて、$k_Y = \sigma_Y \Sigma_{i \in \{1, \cdots, N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$の関係を満たす主情報$k_Y$を計算する（ステップＡ２）。計算された主情報$k_Y$は記憶部４に格納される。

[0097] 導出情報生成部３は、上記生成された乱数σ_{Yj}を用いて、$k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1, \cdots, N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$の関係を満たす導出情報$k_{Yj}$を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）ごとに計算する（ステップＡ３）。計算された導出情報k_{Yj}は記憶部４に格納される。

[0098] ＜情報導出＞

情報生成装置及び方法は、図３のステップＢ１からステップＢ３において、ｕ≦ｖとして、上位のインデックスｖに対応する情報K_vから、下位のインデックスｕに対応する情報K_uを生成する。

[0099] インデックスｖに対応する情報K_vは、主情報k_vと導出情報k_{vj}を含む。主情報k_vは、述語暗号において例えば復号鍵として使用される。導出情報k_{vj}は、インデックスｖに対応する情報K_vよりも下位の情報を生成するために用いられる。例えば、インデックスｖ＝Ｙであり、情報K_v＝情報K_Yである。また、ステップＢ１からステップＢ３の処理により生成された情報K_uを新たな情報K_vとして、インデックスｕに対応する情報K_uよりも下位の情報$K_{u'}$（ｕ’≦ｕ）を生成してもよい。

[0100] インデックスｕに対応する情報K_uは、主情報k_uと導出情報k_{uj}を含む。主情報k_uは、述語暗号において例えば復号鍵として使用される。導出情報k_{uj}は、インデックスｕに対応する情報K_uよりも下位の情報を生成するために用いられる。

情報生成装置には、インデックスｖ及びインデックスｕが入力される。

記憶部４には、インデックスｖに対応する情報K_vが格納されているとする。

[0101] 乱数生成部１は、乱数$\sigma_u \in Z_q$及び集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）に対応する乱数$\sigma_{uj} \in Z_q$を生成する（ステップＢ１）。生成された乱数σ_uは主情報導出部５に送られ、生成された乱数σ_{uj}は導出情報導出部６に送られる。

[0102] 主情報導出部５は、記憶部４から読み込んだ主情報k_v、導出情報k_{vi}及び上記生成された乱数σ_uを用いて、$k_u = \sigma_u \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_v$の関係を満たす、インデックスｕに対応する主情報$k_u$を計算する（ステップＢ２）。計算された主情報$k_u$は、記憶部４に格納される。

[0103] 導出情報導出部６は、記憶部４から読み込んだ導出情報k_{vj}及び上記生成された乱数σ_{uj}を用いて、$k_{uj} = \sigma_{uj} \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_{vj}$の関係を満たすインデックスｕに対応する導出情報$k_{uj}$を集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）ごとに計算する（ステップＢ３）。計算された導出情報k_{uj}は、記憶部４に格納される。

[0104] このようにして、インデックスＹに対応する情報K_Yを生成して、この情報K_Yを基にして下位のインデックスに対応する情報を導出することにより、共通の子ノードＣを持つ親ノードＡと親ノードＢに対して、親ノードＡの情報から共通の子ノードＣの情報を導出し、親ノードＢの情報から共通の子ノードＣの情報を導出することができる。

[0105] ＜具体例１＞

以下、各ノードの情報が述語暗号における鍵であり、インデックスv^1の情報から生成したインデックスv^3の情報と、インデックスv^2の情報から生成したインデックスv^3の情報とが、述語暗号における鍵という観点から一致することを説明する。以下に示すインデックスv^1、インデックスv^2、インデックスv^3は一例であり、他のインデックスについても同様のことが言える。

[0106] インデックスv^1＝｛v_1，v_2，＊，＊｝とし、インデックスv^2＝｛＊，＊，v_3，v_4｝とし、インデックスv^3＝｛v_1，v_2，v_3，v_4｝とする。

定義より、$v^1 \geqq v^3$、$v^2 \geqq v^3$であり、親ノードであるインデックスv^1及び親ノードであるインデックスv^2は、インデックスv^3を共通する子ノードとして有する。なお、以下では、v^i（i＝1，2，3）をv^iと表記することもある。また、インデックスv^iのj番目の要素をv^ijと表記することもある。

[0107] N＝5として、N個の基底b_1^*，b_2^*，b_3^*，b_4^*，b_5^*から、インデックスv^1に対応する情報K_{v^1}及びインデックスv^2に対応する情報K_{v^2}を生成する。σ_{v^1}、σ_{v^13}、σ_{v^14}、σ_{v^2}、σ_{v^23}、σ_{v^24}、σ_{v^3}、σ_{v^3}'は乱数生成部１により生成される乱数である。

[0108] インデックスv^1に対応する情報K_{v^1}（主情報k_{v^1}、導出情報k_{v^13}、k_{v^14}）は以下のようになる。

$$k_{v^1}=\sigma_{v^1}(v_1b_1^*+v_2b_2^*)+b_5^*$$

$$k_{v^13}=\sigma_{v^13}(v_1b_1^*+v_2b_2^*)+b_3^*$$

$$k_{v^14}=\sigma_{v^14}(v_1b_1^*+v_2b_2^*)+b_4^*$$

[0109] また、インデックスv^2に対応する情報K_{v^2}（主情報k_{v^2}、導出情報k_{v^21}、k_{v^22}）は以下のようになる。

$$k_{v^2}=\sigma_{v^2}(v_3b_3^*+v_4b_4^*)+b_5^*$$

$$k_{v^21}=\sigma_{v^23}(v_3b_3^*+v_4b_4^*)+b_1^*$$

$$k_{v^22}=\sigma_{v^24}(v_3b_3^*+v_4b_4^*)+b_2^*$$

[0110] インデックスv^1に対応する情報K_{v^1}からインデックスv^3に対応する主情報k_{v^3}を導出すると以下のようになる。以下の式において、$a=(\sigma_{v^3}(v_3\sigma_{v^13}+v_4\sigma_{v^14})+\sigma_{v1})$であり、$b=\sigma_{v^3}$である。

$$k_{v^3}=\sigma_{v^3}(v_3k_{v^13}+v_4k_{v^14})+k_{v^1}$$

$$=(\sigma_{v^3}(v_3\sigma_{v^13}+v_4\sigma_{v^14})+\sigma_{v^1})(v_1b_1^*+v_2b_2^*)+\sigma_{v^3}(v_3b_3^*+v_4b_4^*)+b_5^*$$

$$=a(v_1b_1^*+v_2b_2^*)+b(v_3b_3^*+v_4b_4^*)+b_5^*$$

…（A）

[0111] インデックスv^2に対応する情報K_{v^2}からインデックスv^3に対応する主情

報$k_{v\hat{}3}$を導出すると以下のようになる。以下の式において、$c=\sigma_{v\hat{}3}'$であり、$d=(\sigma_{v\hat{}3}'(v_1\sigma_{v\hat{}23}+v_4\sigma_{v\hat{}24})+\sigma_{v\hat{}2})$である。

$$k_{v\hat{}3}=\sigma_{v\hat{}3}'(v_1k_{v\hat{}21}+v_2k_{v\hat{}22})+k_{v\hat{}2}$$

$$=(\sigma_{v\hat{}3}'(v_1\sigma_{v\hat{}23}+v_4\sigma_{v\hat{}24})+\sigma_{v\hat{}2})(v_3b_3^*+v_4b_4^*)+\sigma_{v\hat{}3}'(v_1b_1^*+v_2b_2^*)+b_5^*$$

$$=c(v_1b_1^*+v_2b_2^*)+d(v_3b_3^*+v_4b_4^*)+b_5^* \quad \cdots(B)$$

[0112] 上記（A）式に示した情報$K_{v\hat{}1}$から導出した主情報$k_{v\hat{}3}$と、上記（B）式に示した情報K_{v2}から導出した主情報k_{v3}とを比較すると、値は一致しないが、述語暗号において同値な鍵となる。すなわち、$(v_1b_1^*+v_2b_2^*)$をベクトル(b_1^*, b_2^*)とベクトル(v_1, v_2)の内積と見ると、ベクトル(b_1^*, b_2^*)に対するベクトル(v_1, v_2)の方向が（A）式と（B）式で一致しており、同様に、$(v_3b_3^*+v_4b_4^*)$をベクトル(b_3^*, b_4^*)とベクトル(v_3, v_4)の内積と見ると、ベクトル(b_3^*, b_4^*)に対するベクトル(v_3, v_4)の方向が（A）式と（B）式で一致しており、両鍵は述語暗号において同値な鍵となる。

[0113] ［第二実施形態］

図４に、第二実施形態の情報生成装置の機能ブロック図を例示する。

[0114] G、G_Tを素数位数qの巡回群とし、gを巡回群Gの生成元とし、巡回群Gには$g_T=e(g, g)$が巡回群G_Tの生成元となるようなペアリング関数$e: G\times G\rightarrow G_T$が存在するとし、aを$Z_p$からランダムに選択された乱数とし、gと$g_1=g^a\in G$と巡回群Gからランダムに選択された$g_2, g_3, h_1, \cdots, h_{N-1}\in G$とが公開鍵として公開されているとする。

[0115] ＜情報生成＞

情報生成装置及び方法は、図５のステップＣ１からステップＣ４において、公開鍵を用いてインデックスＹに対応する情報K_Yを生成する。情報K_Yは、第一主情報k_Yと第二主情報g^{r_Y}と導出情報k_{Yj}とを含む。第一主情報k_Y及び第二主情報g^{r_Y}は、例えば復号鍵として使用される。導出情報k_{Yi}は、

インデックスＹに対応する情報K_Yよりも下位の情報を生成するために用いられる。

[0116] 情報生成装置には、インデックス$Y \in I$が入力される。

乱数生成部１は、乱数$r_Y \in Z_q$を生成する（ステップＣ１）。生成された乱数r_Yは、第一主情報生成部２１、第二主情報生成部２２及び導出情報生成部３に送られる。

[0117] 第一主情報生成部２１は、上記生成された乱数r_Yを用いて、$k_Y = g_2^{a}$（$g_3 \prod_{i \in \{1, \cdots, N-1\} \setminus w(Y)} h_i^{Yi}$）^{r_Y}の関係を満たす第一主情報$k_Y$を計算する（ステップＣ２）。計算された第一主情報$k_Y$は記憶部４に格納される。

第二主情報生成部２２は、上記生成された乱数r_Yを用いて、第二主情報g^{r_Y}を計算する（ステップＣ３）。計算された第二主情報k_Yは記憶部４に格納される。

[0118] 導出情報生成部３は、上記生成された乱数r_Yを用いて、$k_{Yj} = h_j^{r_Y}$の関係を満たす導出情報k_{Yj}を集合ｗ（Ｙ）の各要素$j \in w(Y)$ごとに計算する（ステップＣ４）。計算された導出情報k_{Yi}は、記憶部４に格納される。

[0119] ＜情報導出＞

情報生成装置及び方法は、図６のステップＤ１からステップＤ４において、$u \leqq v$として、上位のインデックスｖに対応する情報K_vから、下位のインデックスｕに対応する情報K_uを生成する。

[0120] インデックスｖに対応する情報K_vは、第一主情報k_vと第二主情報g^{r_v}と導出情報k_{vj}とを含む。第一主情報k_v及び第二主情報g^{r_v}は、例えば復号鍵として使用される。導出情報k_{vj}は、インデックスｖに対応する情報K_vよりも下位の情報を生成するために用いられる。例えば、インデックス$v = Y$であり、情報K_v＝情報K_Yである。また、ステップＤ１からステップＤ４の処理により生成された情報K_uを新たな情報K_vとして、インデックスｕに対応する情報K_uよりも下位の情報$K_{u'}$（$u' \leqq u$）を生成してもよい。

[0121] インデックスｕに対応する情報K_uは、第一主情報k_uと第二主情報g^{r_u}と導出情報k_{uj}とを含む。第一主情報k_u及び第二主情報g^{r_u}は、例えば復号鍵

として使用される。導出情報k_{uj}は、インデックスｕに対応する情報K_uよりも下位の情報を生成するために用いられる。

[0122] 情報生成装置には、インデックスｖ及びインデックスｕが入力される。

記憶部４には、インデックスｖに対応する情報K_vが格納されているとする。

乱数生成部１は、乱数r_uを生成する（ステップＤ１）。生成された乱数は、第一主情報導出部５１、第二主情報導出部５２及び導出情報導出部６に送られる。

[0123] 第一主情報導出部５１は、上記生成された乱数r_u、記憶部４から読み込んだ第一主情報k_v及び導出情報k_{vi}を用いて、$k_u = k_v (\Pi_{i \in w(v) \setminus w(u)} k_{vi}^{ui}) (g^3 \Pi_{i \in \{1, \cdots, N-1\} \setminus w(v)} h_i^{vi} \Pi_{i \in w(v) \setminus w(u)} h_i^{ui})^{ru}$の関係を満たす、インデックスｕに対応する第一主情報k_uを計算する（ステップＤ２）。計算された第一主情報k_uは、記憶部４に格納される。

[0124] 第二主情報導出部５２は、上記生成された乱数r_uを用いて、第二主情報g^{ru}を計算する（ステップＤ３）。計算された第二主情報g^{ru}は、記憶部４に格納される。

[0125] 導出情報導出部６は、上記記憶部から読み込んだ導出情報k_{vi}及び上記生成された乱数r_uを用いて、$k_{uj} = k_{vj} h_j^{ru}$の関係を満たす導出情報k_{uj}を集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）ごとに計算する（ステップＤ４）。計算された導出情報k_{uj}は、記憶部４に記憶される。

[0126] このようにして、インデックスＹに対応する情報K_Yを生成して、この情報K_Vを基にして下位のインデックスに対応する情報を導出することにより、共通の子ノードＣを持つ親ノードＡと親ノードＢに対して、親ノードＡの情報から共通の子ノードＣの情報を導出し、親ノードＢの情報から共通の子ノードＣの情報を導出することができる。

[0127] ＜具体例２＞

以下、各ノードの情報が述語暗号における鍵であり、インデックスv^1の情報から生成したインデックスv^3の情報と、インデックスv^2の情報から生成

したインデックスv^3の情報とが、述語暗号における鍵という観点から一致することを説明する。以下に示すインデックスv^1、インデックスv^2、インデックスv^3は一例であり、他のインデックスについても同様のことが言える。

[0128] インデックスv^1＝｛v_1，v_2，＊，＊｝とし、インデックスv^2＝｛＊，＊，v_3，v_4｝とし、インデックスv^3＝｛v_1，v_2，v_3，v_4｝とする。定義より、$v^1 \geqq v^3$、$v^2 \geqq v^3$であり、親ノードであるインデックスv^1及び親ノードであるインデックスv^2は、インデックスv^3を共通する子ノードとして有する。なお、以下では、v^i（ｉ＝１，２，３）をｖ＾ｉと表記することもある。また、インデックスv^iのｊ番目の要素をｖ＾ｉｊと表記することもある。

[0129] Ｎ＝５として、$g_1 = g^a$，g_2，g_3，h_1，h_2，h_3，$h_4 \in G$が公開鍵として公開されているとする。これらの公開鍵から、インデックスv^1に対応する情報$K_{v\hat{}1}$及びインデックスv^2に対応する情報$K_{v\hat{}2}$を生成する。$r_{v\hat{}1}$、$r_{v\hat{}2}$は乱数生成部１により生成される乱数である。

[0130] インデックスv^1に対応する情報$K_{v\hat{}1}$（第一主情報$k_{v\hat{}1}$、第二主情報$g^{r_{v\hat{}1}}$、導出情報$k_{v\hat{}13}$、$k_{v\hat{}14}$）は以下のようになる。

$k_{v\hat{}1} = g_2^{a}\,(g_3 h_1^{v1} h_2^{v2})^{r_{v\hat{}1}}$

$g^{r_{v\hat{}1}}$

$k_{v\hat{}13} = h_3^{r_{v\hat{}1}}$

$k_{v\hat{}14} = h_4^{r_{v\hat{}1}}$

[0131] また、インデックスv^2に対応する情報$K_{v\hat{}2}$（第一主情報$k_{v\hat{}2}$、第二導出情報$g^{r_{v\hat{}2}}$、導出情報$k_{v\hat{}21}$、$k_{v\hat{}22}$）は以下のようになる。

$k_{v\hat{}2} = g_2^{a}\,(g_3 h_3^{v3} h_4^{v4})^{r_{v\hat{}2}}$

$g^{r_{v\hat{}2}}$

$k_{v\hat{}21} = h_1^{r_{v\hat{}2}}$

$k_{v\hat{}22} = h_2^{r_{v\hat{}2}}$

[0132] インデックスv^1に対応する情報$K_{v\hat{}1}$からインデックスv^3に対応する第一主情報$k_{v\hat{}3}$を導出すると以下のようになる。なお、$r_{v\hat{}3}$は乱数生成部１に

より生成される乱数であり、$r = r_{v^1} + r_{v^3}$である。

$$k_{v^3} = k_{v^1}(k_{v^{13}}{}^{v^3} k_{v^{14}}{}^{v^4})(g_3 h_1{}^{v^1} h_2{}^{v^2} h_3{}^{v^3} h_4{}^{v^4})^{r_{v^3}}$$

$$= g_2{}^{a}\ (g_3 h_1{}^{v^1} h_2{}^{v^2} h_3{}^{v^3} h_4{}^{v^4})^{r} \quad \cdots (C)$$

インデックスv^2に対応する情報K_{v^2}からインデックスv^3に対応する主情報k_{v^3}を導出すると以下のようになる。なお、$r_{v^{3'}}$は乱数であり、$r' = r_{v^2} + r_{v^{3'}}$である。

$$k_{v^3} = k_{v^2}(k_{v^{21}}{}^{v^1} k_{v^{22}}{}^{v^2})(g_3 h_1{}^{v^1} h_2{}^{v^2} h_3{}^{v^3} h_4{}^{v^4})^{r_{v^{3'}}}$$

$$= g_2{}^{a}\ (g_3 h_1{}^{v^1} h_2{}^{v^2} h_3{}^{v^3} h_4{}^{v^4})^{r'} \quad \cdots (D)$$

[0133] 上記（C）式に示した情報K_{v^1}から導出した第一主情報k_{v^3}及び第二主情報$g^{r_{v^3}}$と、上記（D）式に示した情報K_{v^2}から導出した第一主情報k_{v^3}及び第二主情報$g^{r_{v^{3'}}}$とを比較すると、これらの値は一致しないが、公開鍵g_3，h_1，h_2，h_3，h_4の指数の比が一致しており、述語暗号において同値な鍵となる。

[0134] ［変形例等］

上記の実施形態では、情報生成装置は、主情報生成部２、導出情報生成部３、主情報導出部５及び導出情報導出部６の全てを有していたが、これらの少なくとも１つの部を有していればよい。例えば、主情報生成部２及び導出情報生成部３のみを有していてもよい。また、主情報導出部５及び導出情報導出部６のみを有しており、既に生成され記憶部４に格納された情報K_vを用いて、情報K_uを生成してもよい。

[0135] また、上述の有限体F_q上で定義された各演算を位数qの有限環Z_q上で定義された演算に置き換えてもよい。有限体F_q上で定義された各演算を有限環Z_q上で定義された演算に置き換える方法の一例は、素数やそのべき乗値以外のqを許容する方法である。

[0136] 情報生成装置は、コンピュータによって実現することができる。この場合、これらの装置がそれぞれ有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、これらの装置における各処理機能が、コンピュータ上で実現される。

[0137] この処理内容を記述した情報生成プログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、これらの装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

[0138] この発明は、上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。

請求の範囲

[請求項1] ｅが巡回群G_1のＮ個の元γ_L（Ｌ＝１，…，Ｎ）（Ｎ≧２）と巡回群G_2のＮ個の元γ_L^*（Ｌ＝１，…，Ｎ）との入力に対して巡回群G_Tの１個の元を出力する非退化な双線形関数であり、$b_i \in G_1^N$（ｉ＝１，…，Ｎ）のそれぞれが、上記巡回群G_1のＮ個の元を要素とするＮ次元の基底ベクトルであり、$b_j^* \in G_2^N$（ｊ＝１，…，Ｎ）のそれぞれが、上記巡回群G_2のＮ個の元を要素とするＮ次元の基底ベクトルであり、上記基底ベクトル$b_i \in G_1^N$（ｉ＝１，…，Ｎ）の各要素と上記基底ベクトル$b_j^* \in G_2^N$（ｊ＝１，…，Ｎ）の各要素とを上記双線形関数ｅに入力して得られる関数値が、ｉ＝ｊの場合に$\delta(i, j) = 1_F$となってｉ≠ｊの場合に$\delta(i, j) = 0_F$となるクロネッカーのデルタ関数$\delta(i, j)$を用いて$g_T^{\tau \cdot \delta(i, j)} \in G_T$と表現され、$0_F$が有限体$F_q$の加法単位元であり、$1_F$が有限体$F_q$の乗法単位元であり、$\tau$が$0_F$を除く有限体$F_q$の元であり、$g_T$が上記巡回群$G_T$の生成元であり、

＊を不定文字とし、インデックスＹをＹ＝（Y_1，…，Y_{N-1}）∈Ｉ＝（$F_q \cup \{*\}$）$^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜Y_i＝＊｝として、

乱数$\sigma_Y \in Z_q$、及び、集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）に対応する乱数$\sigma_{Yj} \in Z_q$を生成する乱数生成部と、

上記生成された乱数σ_Yを用いて、$k_Y = \sigma_Y \Sigma_{i \in [1, \cdots, N-1] \setminus w(Y)} Y_i b_i^* + b_N^*$の関係を満たす主情報$k_Y$を計算する主情報生成部と、

上記生成された乱数σ_{Yj}を用いて、$k_{Yj} = \sigma_{Yj} \Sigma_{i \in [1, \cdots, N-1] \setminus w(Y)} Y_i b_i^* + b_j^*$の関係を満たす導出情報$k_{Yj}$を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）ごとに計算する導出情報生成部と、

を含むことを特徴とする情報生成装置。

[請求項2] 請求項１に記載の情報生成装置において、

＊を不定文字とし、インデックスｖをｖ＝（v_1，…，v_{N-1}）∈Ｉ＝（F_qＵ｛＊｝）$^{N-1}$とし、インデックスｖに対応する集合ｗ（ｖ）をｗ（ｖ）＝｛ｉ｜v_i＝＊｝とし、インデックスｕをｕ＝（u_1，…，u_{N-1}）∈Ｉ＝（F_qＵ｛＊｝）$^{N-1}$とし、インデックスｕに対応する集合ｗ（ｕ）をｗ（ｕ）＝｛ｉ｜u_i＝＊｝とし、集合ｗ（ｕ）⊂集合ｗ（ｖ）とし、v_i＝u_i（ｉ∈｛１，…，Ｎ－１｝＼ｗ（ｖ））として、

インデックスｖに対応する主情報k_v及びインデックスｖに対応する導出情報k_{vj}を記憶する記憶部と、

上記乱数生成部は、更に乱数$\sigma_u \in Z_q$を生成し、

上記記憶部から読み込んだ主情報k_v、導出情報k_{vi}及び上記生成された乱数σ_uを用いて、$k_u=\sigma_u \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_v$の関係を満たす、インデックスｕに対応する主情報$k_u$を計算する主情報導出部と、

を含む情報生成装置。

[請求項3] 請求項２に記載の情報生成装置において、

上記乱数生成部は、更に集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）に対応する乱数$\sigma_{uj} \in Z_q$を生成し、

上記記憶部から読み込んだ導出情報k_{vj}及び上記生成された乱数σ_{ui}を用いて、$k_{uj}=\sigma_{uj} \Sigma_{i\in w(v)\setminus w(u)} u_i k_{vi} + k_{vj}$の関係を満たすインデックスｕに対応する導出情報$k_{uj}$を集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）ごとに計算する導出情報導出部を更に含む、

ことを特徴とする情報生成装置。

[請求項4] ｅが巡回群G_1のＮ個の元γ_L（Ｌ＝１，…，Ｎ）（Ｎ≧２）と巡回群G_2のＮ個の元γ_L＊（Ｌ＝１，…，Ｎ）との入力に対して巡回群G_Tの１個の元を出力する非退化な双線形関数であり、$b_i \in G_1^N$（ｉ＝１，…，Ｎ）のそれぞれが、上記巡回群G_1のＮ個の元を要素とするＮ次元の基底ベクトルであり、$b_j^* \in G_2^N$（ｊ＝１，…，Ｎ）

のそれぞれが、上記巡回群G_2のＮ個の元を要素とするＮ次元の基底ベクトルであり、上記基底ベクトル$b_i \in G_1^N$（ｉ＝１，…，Ｎ）の各要素と上記基底ベクトル$b_j^* \in G_2^N$（ｊ＝１，…，Ｎ）の各要素とを上記双線形関数ｅに入力して得られる関数値が、ｉ＝ｊの場合にδ（ｉ，ｊ）＝1_Fとなってｉ≠ｊの場合にδ（ｉ，ｊ）＝0_Fとなるクロネッカーのデルタ関数δ（ｉ，ｊ）を用いて$g_T^{\tau \cdot \delta(i,j)} \in G_T$と表現され、$0_F$が有限体$F_q$の加法単位元であり、$1_F$が有限体$F_q$の乗法単位元であり、$\tau$が$0_F$を除く有限体$F_q$の元であり、$g_T$が上記巡回群$G_T$の生成元であり、

＊を不定文字とし、インデックスＹをＹ＝（Y_1，…，Y_{N-1}）∈Ｉ＝（$F_q \cup \{*\}$）$^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜Y_i＝＊｝とし、$\sigma_Y \in Z_q$を乱数とし、σ_{Yi}を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）に対応する乱数とし、インデックスＹに対応する主情報k_Yは$k_Y = \sigma_Y \Sigma_{i \in \{1,\cdots,N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$の関係を満たし、インデックスＹに対応する導出情報$k_{Yi}$は$k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1,\cdots,N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$の関係を満たし、

＊を不定文字とし、インデックスｖをｖ＝（v_1，…，v_{N-1}）∈Ｉ＝（$F_q \cup \{*\}$）$^{N-1}$とし、インデックスｕをｕ＝（u_1，…，u_{N-1}）∈Ｉ＝（$F_q \cup \{*\}$）$^{N-1}$とし、インデックスｖに対応する集合ｗ（ｖ）をｗ（ｖ）＝｛ｉ｜v_i＝＊｝とし、インデックスｕに対応する集合ｗ（ｕ）をｗ（ｕ）＝｛ｉ｜u_i＝＊｝とし、集合ｗ（ｕ）⊂集合ｗ（ｖ）とし、$v_i = u_i$（ｉ∈｛１，…，Ｎ－１｝＼ｗ（ｖ））として、

上記主情報k_Yである又は上記主情報k_Y及び上記導出情報k_{Yi}から導出されたインデックスｖに対応する主情報k_v、及び、上記導出情報k_{Yi}である又は上記導出情報k_{Yi}から導出されたインデックスｖに対応する導出情報k_{vj}を記憶する記憶部と、

乱数$\sigma_u \in Z_q$を生成する子乱数生成部と、

上記記憶部から読み込んだ主情報k_v、導出情報k_{vi}及び上記生成された乱数σ_uを用いて、$k_u = \sigma_u \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_v$の関係を満たす、インデックスuに対応する主情報$k_u$を計算する主情報導出部と、

を含む情報生成装置。

[請求項5] 請求項４に記載の情報生成装置において、

上記乱数生成部は、さらに集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）に対応する乱数$\sigma_{uj} \in Z_q$を生成し、

上記記憶部から読み込んだ導出情報k_{vj}及び上記生成された乱数σ_{ui}を用いて、$k_{uj} = \sigma_{uj} \Sigma_{i \in w(v) \setminus w(u)} u_i k_{vi} + k_{vj}$の関係を満たす導出情報$k_{uj}$を集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）ごとに計算する導出情報導出部を更に含む、

ことを特徴とする情報生成装置。

[請求項6] Ｇ、G_Tを素数位数ｑの巡回群とし、ｇを巡回群Ｇの生成元とし、巡回群Ｇには$g_T = e(g, g)$が巡回群G_Tの生成元となるようなペアリング関数ｅ：Ｇ×Ｇ→G_Tが存在するとし、ａをZ_pからランダムに選択された乱数とし、ｇと$g_1 = g^a \in G$と巡回群Ｇからランダムに選択されたg_2，g_3，h_1，…，$h_{N-1} \in G$とが公開鍵として公開されており、

＊を不定文字とし、インデックスＹをＹ＝（Y_1，…，Y_{N-1}）∈Ｉ＝（$F_q \cup \{*\}$）$^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜Y_i＝＊｝として、

乱数$r_Y \in Z_q$を生成する乱数生成部と、

上記生成された乱数r_Yを用いて、$k_Y = g_2^a (g_3 \Pi_{i \in [1, \cdots, N-1] \setminus w(Y)} h_i^{Yi})^{rY}$の関係を満たす第一主情報$k_Y$を計算する第一主情報生成部と、

上記生成された乱数r_Yを用いて、第二主情報g^{rY}を計算する第二

主情報生成部と、

上記生成された乱数r_Yを用いて、$k_{Yj}=h_j{}^{r_Y}$の関係を満たす導出情報k_{Yj}を集合w（Y）の各要素$j\in w(Y)$ごとに計算する導出情報生成部と、

を含むことを特徴とする情報生成装置。

[請求項7] 請求項６に記載の情報生成装置において、

上記乱数生成部は、更に乱数$r_u\in Z_q$を生成し、

＊を不定文字とし、インデックスvを$v=(v_1,\cdots,v_{N-1})\in I=(F_q\cup\{*\})^{N-1}$とし、インデックスvに対応する集合w（v）をw（v）＝｛i｜$v_i=*$｝とし、インデックスuを$u=(u_1,\cdots,u_{N-1})\in I=(F_q\cup\{*\})^{N-1}$とし、インデックスuに対応する集合w（u）をw（u）＝｛i｜$u_i=*$｝とし、集合w（u）⊂集合w（v）とし、$v_i=u_i$（$i\in\{1,\cdots,N-1\}\setminus w(v)$）として、

インデックスvに対応する第一主情報k_v、第二主情報g^r及びインデックスvに対応する導出情報k_{vj}を記憶する記憶部と、

上記記憶部から読み込んだ第一主情報k_v及び導出情報k_{vi}を用いて、$k_u=k_v(\prod_{i\in w(v)\setminus w(u)}k_{vi}{}^{u_i})(g_3\prod_{i\in\{1,\cdots,N-1\}\setminus w(v)}h_i{}^{v_i}\prod_{i\in w(v)\setminus w(u)}h_i{}^{u_i})^{r_u}$の関係を満たす、インデックスuに対応する第一主情報k_uを計算する第一主情報導出部と、

上記生成された乱数r_uを用いて、第二主情報g^{r_u}を計算する第二主情報導出部と、

を含むことを特徴とする情報生成装置。

[請求項8] 請求項７に記載の情報生成装置において、

上記記憶部から読み込んだ導出情報k_{vi}及び上記生成された乱数r_uを用いて、$k_{uj}=k_{vj}h_j{}^{r_u}$の関係を満たす導出情報k_{uj}を集合w（u）の各要素$j\in w(u)$ごとに計算する導出情報導出部を更に含む、

ことを特徴とする情報生成装置。

[請求項9] Ｇ、G_Tを素数位数ｑの巡回群とし、ｇを巡回群Ｇの生成元とし、巡回群Ｇには$g_T = e(g, g)$が巡回群G_Tの生成元となるようなペアリング関数ｅ：$G \times G \to G_T$が存在するとし、ａをZ_pからランダムに選択された乱数とし、ｇと$g_1 = g^a \in G$と巡回群Ｇからランダムに選択されたg_2，g_3，h_1，…，$h_{N-1} \in G$とが公開鍵として公開されており、

＊を不定文字とし、インデックスＹを$Y = (Y_1, \cdots, Y_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜$Y_i = *$｝とし、

$r_Y \in Z_q$を乱数とし、インデックスＹに対応する第一主情報k_Yは$k_Y = g_2^a (g_3 \prod_{i \in \{1, \cdots, N-1\} \setminus w(Y)} h_i^{Y_i})^{r_Y}$の関係を満たし、$g^{r_Y}$をインデックスＹに対応する第二主情報とし、インデックスＹに対応する導出情報k_{Y_i}は$k_{Y_j} = h_j^{r_Y}$の関係を満たし、

＊を不定文字とし、インデックスｖを$v = (v_1, \cdots, v_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$とし、インデックスｖに対応する集合ｗ（ｖ）をｗ（ｖ）＝｛ｉ｜$v_i = *$｝とし、インデックスｕを$u = (u_1, \cdots, u_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$とし、インデックスｕに対応する集合ｗ（ｕ）をｗ（ｕ）＝｛ｉ｜$u_i = *$｝とし、集合ｗ（ｕ）⊂集合ｗ（ｖ）とし、$v_i = u_i$（ｉ∈｛１，…，Ｎ－１｝＼ｗ（ｖ））として、

乱数$r_u \in Z_q$を生成する乱数生成部と、

上記第一主情報k_Yである又は上記第一主情報k_Y及び上記導出情報k_{Y_i}から導出されたインデックスｖに対応する第一主情報k_v、上記導出情報k_{Y_i}である又は上記導出情報k_{Y_i}から導出されたインデックスｖに対応する導出情報k_{v_j}を記憶する記憶部と、

上記記憶部から読み込んだ第一主情報k_v及び上記導出情報k_{v_i}を用いて、$k_u = k_v (\prod_{i \in w(v) \setminus w(u)} k_{v_i}^{u_i}) (g_3 \prod_{i \in \{1, \cdots, N-1\}}$

$\setminus_{w(v)} h_i^{v_i} \prod_{i \in w(v) \setminus w(u)} h_i^{u_i})^{r_u}$の関係を満たす、インデックスｕに対応する第一主情報k_uを計算する第一主情報導出部と、

上記生成された乱数r_uを用いて、第二主情報g^{r_u}を計算する第二主情報導出部と、

を含む情報生成装置。

[請求項10] 請求項９に記載された情報生成装置において、

上記記憶部から読み込んだ導出情報k_{v_i}及び上記生成された乱数r_uを用いて、$k_{u_j} = k_{v_j} h_j^{r_u}$の関係を満たす導出情報$k_{u_j}$を集合ｗ（ｕ）の各要素ｊ∈ｗ（ｕ）ごとに計算する導出情報導出部を更に含む、

情報生成装置。

[請求項11] ｅが巡回群G_1のＮ個の元γ_L（Ｌ＝１，…，Ｎ）（Ｎ≧２）と巡回群G_2のＮ個の元γ_L^*（Ｌ＝１，…，Ｎ）との入力に対して巡回群G_Tの１個の元を出力する非退化な双線形関数であり、$b_i \in G_1^N$（ｉ＝１，…，Ｎ）のそれぞれが、上記巡回群G_1のＮ個の元を要素とするＮ次元の基底ベクトルであり、$b_j^* \in G_2^N$（ｊ＝１，…，Ｎ）のそれぞれが、上記巡回群G_2のＮ個の元を要素とするＮ次元の基底ベクトルであり、上記基底ベクトル$b_i \in G_1^N$（ｉ＝１，…，Ｎ）の各要素と上記基底ベクトル$b_j^* \in G_2^N$（ｊ＝１，…，Ｎ）の各要素とを上記双線形関数ｅに入力して得られる関数値が、ｉ＝ｊの場合に$\delta(i, j) = 1_F$となってｉ≠ｊの場合に$\delta(i, j) = 0_F$となるクロネッカーのデルタ関数$\delta(i, j)$を用いて$g_T^{\tau \cdot \delta(i, j)} \in G_T$と表現され、$0_F$が有限体$F_q$の加法単位元であり、$1_F$が有限体$F_q$の乗法単位元であり、$\tau$が$0_F$を除く有限体$F_q$の元であり、$g_T$が上記巡回群$G_T$の生成元であり、

＊を不定文字とし、インデックスＹをＹ＝（Y_1，…，Y_{N-1}）∈Ｉ＝（$F_q \cup \{*\}$）$^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜Y_i＝＊｝として、

乱数生成部が、乱数$\sigma_Y \in Z_q$、及び、集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）に対応する乱数$\sigma_{Yj} \in Z_q$を生成する乱数生成ステップと、

主情報生成部が、上記生成された乱数σ_Yを用いて、$k_Y = \sigma_Y \Sigma_{i \in \{1, \cdots, N-1\} \setminus w(Y)} Y_i b_i^* + b_N^*$の関係を満たす主情報$k_Y$を計算する主情報生成ステップと、

導出情報生成部が、上記生成された乱数σ_{Yj}を用いて、$k_{Yj} = \sigma_{Yj} \Sigma_{i \in \{1, \cdots, N-1\} \setminus w(Y)} Y_i b_i^* + b_j^*$の関係を満たす導出情報$k_{Yj}$を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）ごとに計算する導出情報生成ステップと、

を含むことを特徴とする情報生成方法。

[請求項12] Ｇ、G_Tを素数位数ｑの巡回群とし、ｇを巡回群Ｇの生成元とし、巡回群Ｇには$g_T = e(g, g)$が巡回群G_Tの生成元となるようなペアリング関数ｅ：$G \times G \rightarrow G_T$が存在するとし、ａを$Z_p$からランダムに選択された乱数とし、ｇと$g_1 = g^a \in G$と巡回群Ｇからランダムに選択された$g_2$，$g_3$，$h_1$，…，$h_{N-1} \in G$とが公開鍵として公開されており、

＊を不定文字とし、インデックスＹを$Y = (Y_1, \cdots, Y_{N-1}) \in I = (F_q \cup \{*\})^{N-1}$とし、インデックスＹに対応する集合ｗ（Ｙ）をｗ（Ｙ）＝｛ｉ｜$Y_i = *$｝として、

乱数生成部が、乱数$r_Y \in Z_q$を生成する乱数生成ステップと、

第一主情報生成部が、上記生成された乱数r_Yを用いて、$k_Y = g_2^a (g_3 \Pi_{i \in \{1, \cdots, N-1\} \setminus w(Y)} h_i^{Yi})^{r_Y}$の関係を満たす第一主情報$k_Y$を計算する第一主情報生成ステップと、

第二主情報生成部が、上記生成された乱数r_Yを用いて、第二主情報g^{r_Y}を計算する第二主情報生成ステップと、

導出情報生成部が、上記生成された乱数r_Yを用いて、$k_{Yj} = h_j^{r_Y}$の関係を満たす導出情報k_{Yj}を集合ｗ（Ｙ）の各要素ｊ∈ｗ（Ｙ）ごとに計算する導出情報生成ステップと、

を含むことを特徴とする情報生成方法。

[請求項13] 請求項１から１０の何れかに記載された情報生成装置の各部としてコンピュータを機能させるための情報生成プログラム。

[請求項14] 請求項１３に記載された情報生成プログラムを記録したコンピュータ読み取り可能な記録媒体。

[図1]

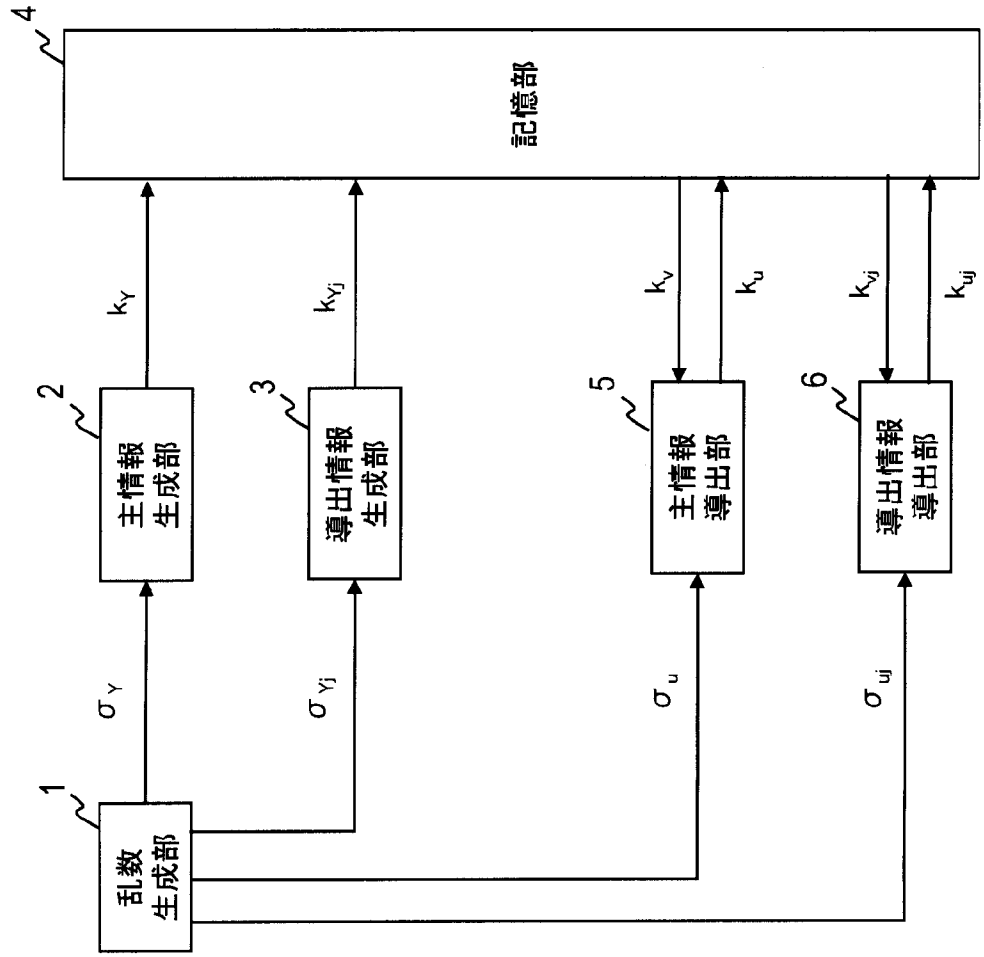
4
記憶部
k_Y
k_{Yj}
k_v
k_u
k_{vj}
k_{uj}
2
主情報
生成部
3
導出情報
生成部
5
主情報
導出部
6
導出情報
導出部
σ_Y
σ_{Yj}
σ_u
σ_{uj}
1
乱数
生成部

図1

[図2]

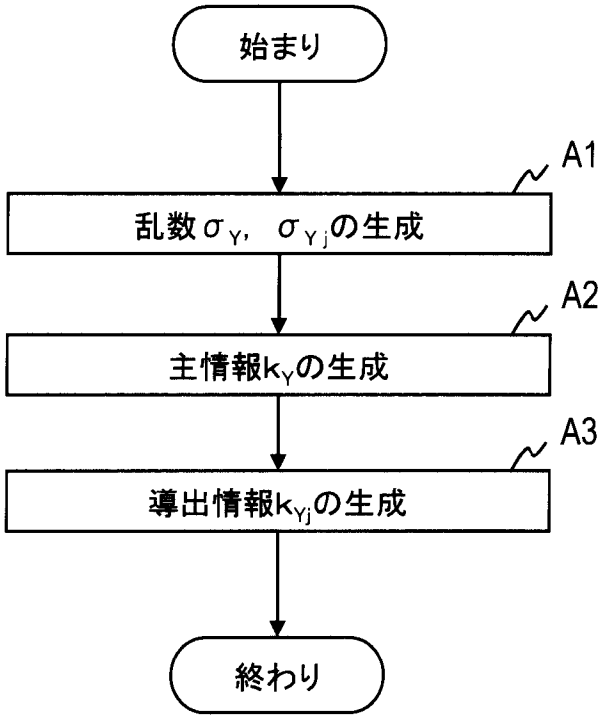
始まり
A1
乱数σ_Y, σ_{Yj}の生成
A2
主情報k_Yの生成
A3
導出情報k_{Yj}の生成
終わり

図２

[図3]

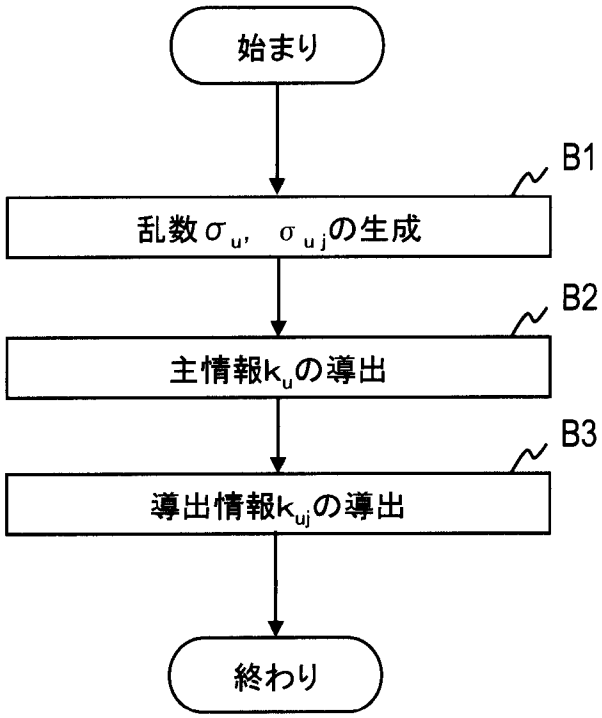
始まり
B1
乱数σ_u, σ_{uj}の生成
B2
主情報k_uの導出
B3
導出情報k_{uj}の導出
終わり

図３

[図4]

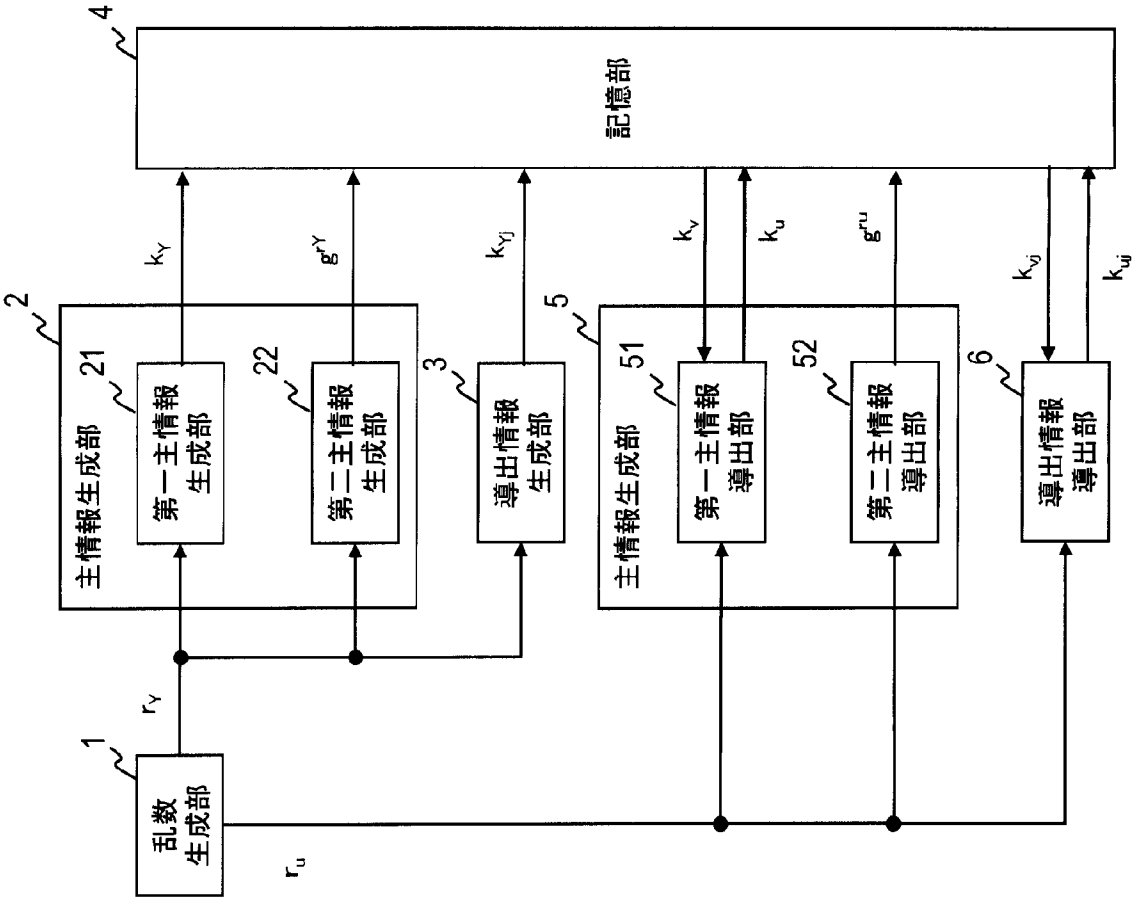
4
記憶部
2
主情報生成部
21
第一主情報生成部
22
第二主情報生成部
3
導出情報生成部
5
主情報生成部
51
第一主情報導出部
52
第二主情報導出部
6
導出情報導出部
1
乱数生成部
k_Y
g^{rY}
k_{Yj}
k_v
k_u
g^{ru}
k_{vj}
k_{uj}
r_Y
r_u

図4

[図5]

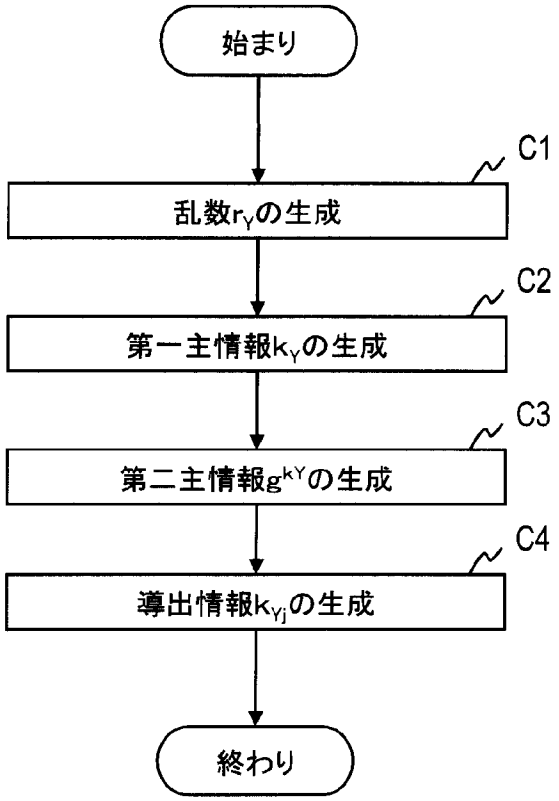
始まり
C1
乱数r_Yの生成
C2
第一主情報k_Yの生成
C3
第二主情報g^{kY}の生成
C4
導出情報k_{Yj}の生成
終わり

図５

[図6]

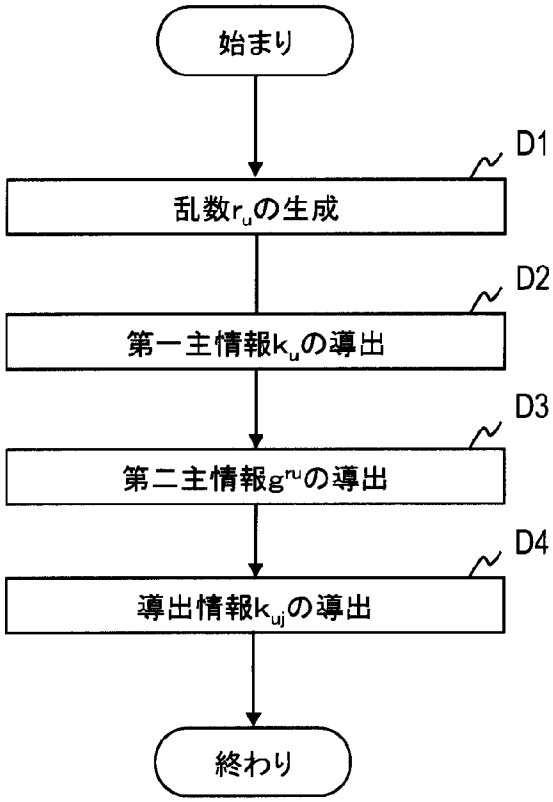
始まり
D1
乱数r_uの生成
D2
第一主情報k_uの導出
D3
第二主情報g^{ru}の導出
D4
導出情報k_{uj}の導出
終わり

図６

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/057279

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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	X. Boyen and B. Waters, Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), [online].Cryptology ePrint Archive, 2006.06.08, Report 2006/085, [retrieved on 2010.05.31]. Retrieved from the Internet: <URL:http://eprint.iacr.org/2006/085>.	1-14
A	J. Katz, A. Sahai, B. Waters, Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, [online]. Cryptology ePrint Archive, 2008.07.08, Report 2007/404, [retrieved on 2010.05.26]. Retrieved from the Internet: <URL:http://eprint.iacr.org/2007/404>.	1-14

☒ 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
31 May, 2010 (31.05.10)	08 June, 2010 (08.06.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/057279

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	E. Shi and B. Waters, Delegating Capabilities in Predicate Encryption Systems, [online]. Cryptology ePrint Archive, 2008.06.24, Report 2008/279, [retrieved on 2010.05.31]. Retrieved from the Internet: <URL:http://eprint.iacr.org/2008/279>.	1-14
A	JP 2005-521323 A (Docomo Communications Laboratories U.S.A. Inc.), 14 July 2005 (14.07.2005), entire text; all drawings & US 2007/0050629 A1 & US 2008/0013722 A1 & US 2003/0179885 A1 & EP 1495573 A & EP 2012459 A1 & WO 2003/081780 A2 & DE 60325575 D & CN 1633774 A & AT 419690 T & CN 101527629 A	1-14
A	WO 2008/099831 A1 (NEC Corp.), 21 August 2008 (21.08.2008), entire text; all drawings & US 2010/0020977 A	1-14
A	T. Okamoto, K. Takashima, Hierarchical Predicate Encryption for Inner-Products, Lecture Notes in Computer Science, 2009.12.01, Vol. 5912, pp.214-231.	1-14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／０５７２７９

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	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０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）

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	X. Boyen and B. Waters, Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), [online]. Cryptology ePrint Archive, 2006.06.08, Report 2006/085, [retrieved on 2010.05.31]. Retrieved from the Internet: <URL: http://eprint.iacr.org/2006/085>.	1-14

☑　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 ３１．０５．２０１０	国際調査報告の発送日 ０８．０６．２０１０
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　４５３８ 金沢　史明 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	J. Katz, A. Sahai, B. Waters, Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products, [online]. Cryptology ePrint Archive, 2008.07.08, Report 2007/404, [retrieved on 2010.05.26]. Retrieved from the Internet: <URL: http://eprint.iacr.org/2007/404>.	1-14
A	E. Shi and B. Waters, Delegating Capabilities in Predicate Encryption Systems, [online]. Cryptology ePrint Archive, 2008.06.24, Report 2008/279, [retrieved on 2010.05.31]. Retrieved from the Internet: <URL: http://eprint.iacr.org/2008/279>.	1-14
A	JP 2005-521323 A (ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド) 2005.07.14, 全文、全図. & US 2007/0050629 A1 & US 2008/0013722 A1 & US 2003/0179885 A1 & EP 1495573 A & EP 2012459 A1 & WO 2003/081780 A2 & DE 60325575 D & CN 1633774 A & AT 419690 T & CN 101527629 A	1-14
A	WO 2008/099831 A1 (日本電気株式会社) 2008.08.21, 全文、全図. & US 2010/0020977 A	1-14
A	T. Okamoto, K. Takashima, Hierarchical Predicate Encryption for Inner-Products, Lecture Notes in Computer Science, 2009.12.01, Vol. 5912, pp.214-231.	1-14