(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7248120号
(P7248120)

(45)発行日　令和5年3月29日(2023.3.29)

(24)登録日　令和5年3月20日(2023.3.20)

(51)国際特許分類
Ｇ０９Ｃ　1/00 (2006.01)

ＦＩ
Ｇ０９Ｃ　1/00　６２０Ｚ

請求項の数　5　（全32頁）

(21)出願番号　特願2021-530426(P2021-530426)
(86)(22)出願日　令和1年7月10日(2019.7.10)
(86)国際出願番号　PCT/JP2019/027330
(87)国際公開番号　WO2021/005748
(87)国際公開日　令和3年1月14日(2021.1.14)
審査請求日　令和3年12月10日(2021.12.10)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100070150
弁理士　伊東 忠彦
(74)代理人　100124844
弁理士　石原 隆治
(72)発明者　富田 潤一
東京都千代田区大手町一丁目５番１号
日本電信電話株式会社内
審査官　青木 重徳

最終頁に続く

(54)【発明の名称】　暗号システム、鍵生成装置、暗号化装置、復号装置、及びプログラム

(57)【特許請求の範囲】

【請求項１】

属性ベース暗号に用いられる公開鍵とマスター秘密鍵とを生成するセットアップ手段と、

前記公開鍵と、属性と前記属性に関する任意の条件式で表されたポリシーとのうちのいずれか一方とを少なくとも入力として、前記属性と前記ポリシーとのうちのいずれか一方が埋め込まれた暗号文を少なくとも生成する暗号化手段と、

前記公開鍵と、前記マスター秘密鍵と、前記属性と前記ポリシーとのうちの前記一方とは異なる他方とを入力として、前記他方が埋め込まれた秘密鍵を生成する鍵生成手段と、

前記公開鍵と、前記暗号文と、前記秘密鍵とを入力として、前記暗号文を復号する復号手段と、

を有し、

前記鍵生成手段は、

前記暗号化手段によって前記ポリシーが埋め込まれた暗号文が生成された場合、前記ポリシー中の同じ属性ラベルの出現回数に依存しない鍵サイズの前記秘密鍵を生成し、

前記暗号化手段は、

前記鍵生成手段によって前記ポリシーが埋め込まれる秘密鍵が生成される場合、前記ポリシー中の同じ属性ラベルの出現回数に依存しない暗号文サイズの前記暗号文を生成する、

ことを特徴とする暗号システム。

【請求項２】

任意の条件式で表されたポリシーを暗号文に埋め込み可能な暗号文ポリシー属性ベース暗

号に用いられる公開鍵とマスター秘密鍵とを生成するセットアップ手段と、
前記公開鍵と、前記マスター秘密鍵と、属性とを入力として、前記属性が埋め込まれた秘密鍵を生成する鍵生成手段と、
を有し、
前記鍵生成手段は、
前記ポリシー中の同じ属性ラベルの出現回数に依存しない鍵サイズの前記秘密鍵を生成する、ことを特徴とする鍵生成装置。
【請求項３】
任意の条件式で表されたポリシーを秘密鍵に埋め込み可能な鍵ポリシー属性ベース暗号に用いられる公開鍵と、属性とを入力として、前記属性が埋め込まれた暗号文を少なくとも生成する暗号化手段、
を有し、
前記暗号化手段は、
前記ポリシー中の同じ属性ラベルの出現回数に依存しない暗号文サイズの前記暗号文を生成する、ことを特徴とする暗号化装置。
【請求項４】
属性ベース暗号に用いられる公開鍵と、属性と前記属性に関する任意の条件式で表されたポリシーとのうちのいずれか一方が埋め込まれた暗号文と、前記属性と前記ポリシーとのうちのいずれか一方とは異なる他方が埋め込まれた秘密鍵とを入力として、前記暗号文を復号する復号手段、
を有し、
前記暗号文に前記ポリシーが埋め込まれている場合、前記秘密鍵の鍵サイズは、前記ポリシー中の同じ属性ラベルの出現回数に依存せず、
前記秘密鍵に前記ポリシーが埋め込まれている場合、前記暗号文の暗号文サイズは、前記ポリシー中の同じ属性ラベルの出現回数に依存しない、ことを特徴とする復号装置。
【請求項５】
コンピュータを、請求項１に記載の暗号システムにおける各手段、請求項２に記載の鍵生成装置における各手段、請求項３に記載の暗号化装置における各手段又は請求項４に記載の復号装置における各手段、として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号システム、鍵生成装置、暗号化装置、復号装置、及びプログラムに関する。
【背景技術】
【０００２】
複雑な復号制御が可能な暗号方式として属性ベース暗号が知られている。属性ベース暗号は、主に、鍵ポリシー属性ベース暗号と暗号文ポリシー属性ベース暗号との２つに分けられる。鍵ポリシー属性ベース暗号では、暗号文には平文の他に属性の情報が埋め込まれており、秘密鍵にはポリシー（属性に対する条件式のようなもの）が埋め込まれる。暗号文を秘密鍵で復号する場合には、暗号文に埋め込まれている属性が、秘密鍵に埋め込まれているポリシーを満たすときのみ復号することができる。他方で、暗号文ポリシー属性ベース暗号は、鍵ポリシー属性ベース暗号の対になるもので、暗号文にポリシーが埋め込まれ、秘密鍵に属性の情報が埋め込まれる。
【０００３】
属性ベース暗号の重要な性質の１つにポリシーの表現力がある。ポリシーの表現力とは、概ね、どの程度きめ細かく復号条件を記述できるかということを指す。きめ細かく復号条件を記述できるほどポリシーの表現力が高いことを表す。一般に、ポリシーは論理式で表現されることが多い。例えば、「（役職＝部長）かつ（部署＝総務部）」等のように表される。これは、役職として部長という属性を持っており、かつ、部署として総務部とい

う属性を持っている場合のみ復号を許すというポリシーである。
【０００４】
ポリシーの表現力に関する項目の１つとして、条件式の中で否定を扱えるかどうかというものがある。すなわち、例えば、「（役職＝部長）かつ（部署≠総務部）」というような条件式を扱えるかどうかというものである。このような形で否定を含む条件式を表現でき、かつ、方式の中で属性集合やポリシーの大きさの制限が掛からない暗号方式として、ＯＴ方式が知られている（例えば非特許文献１参照）。
【先行技術文献】
【非特許文献】
【０００５】
【文献】Okamoto T., Takashima K. (2012) Fully Secure Unbounded Inner-Product and Attribute-Based Encryption. In: Wang X., Sako K. (eds) Advances in Cryptology - ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ＯＴ方式は表現力の高さや、属性集合やポリシーの大きさに制限が掛からないという点で優れている一方で、動作が非効率的であり、鍵生成処理や暗号化処理、復号処理等に時間を要する場合がある。属性ベース暗号はスマートフォン等にも応用可能性があり、比較的計算リソースの小さな機器でも実用的な時間で動作することが望ましい。
【０００７】
また、同じ属性ラベルを多数含むようなポリシーを扱えるようにするためには、ＯＴ方式では属性を埋め込む側の要素数を、同じ属性ラベルの出現回数の最大値に比例して増大させる必要がある。例えば、「（（役職＝部長）かつ（部署＝総務部））または（（役職＝課長）かつ（部署＝経理部））」という条件式を考えると、この条件式の中には役職という属性ラベルと部署という属性ラベルとがそれぞれ２回ずつ含まれている。このような条件式を扱えるようにするためには、もとのＯＴ方式に対して鍵ポリシー属性ベース暗号では暗号文（暗号文ポリシー属性ベース暗号では秘密鍵）の大きさ（サイズ）を２倍にする必要がある。同じ属性ラベルの出現回数がより多い条件式を扱えるようにするためには、暗号文又は秘密鍵のサイズをより大きくしなければならない。
【０００８】
本発明の実施形態は、上記の点に鑑みてなされたもので、暗号文や秘密鍵のサイズを増大させずに任意の条件式をポリシーとして利用可能で、効率的な属性ベース暗号を実現することを目的とする。
【課題を解決するための手段】
【０００９】
上記目的を達成するため、本実施形態に係る暗号システムは、属性ベース暗号に用いられる公開鍵とマスター秘密鍵とを生成するセットアップ手段と、前記公開鍵と、属性と前記属性に関する任意の条件式で表されたポリシーとのうちのいずれか一方とを少なくとも入力として、前記属性と前記ポリシーとのうちのいずれか一方が埋め込まれた暗号文を少なくとも生成する暗号化手段と、前記公開鍵と、前記マスター秘密鍵と、前記属性と前記ポリシーとのうちの前記一方とは異なる他方とを入力として、前記他方が埋め込まれた秘密鍵を生成する鍵生成手段と、前記公開鍵と、前記暗号文と、前記秘密鍵とを入力として、前記暗号文を復号する復号手段と、を有することを特徴とする。
【発明の効果】
【００１０】
暗号文や秘密鍵のサイズを増大させずに任意の条件式をポリシーとして利用可能で、効率的な属性ベース暗号を実現することができる。
【図面の簡単な説明】

【００１１】
【図１】本実施形態に係る暗号システムの全体構成の一例を示す図である。
【図２】本実施形態に係る鍵生成装置、暗号化装置及び復号装置のハードウェア構成の一例を示す図である。
【発明を実施するための形態】
【００１２】
以下、本発明の実施の形態（以降、「本実施形態」とも表す。）について説明する。本実施形態では、暗号文や秘密鍵のサイズを増大させずに任意の条件式をポリシーとして利用可能で、かつ、効率的に動作する属性ベース暗号を実現する暗号システム１について説明する。
【００１３】
＜準備＞
まず、本実施形態の説明に必要な記法や概念等について説明する。
【００１４】
・記法
ｐを素数として、体Ｚ／ｐＺをZ_pと表す。有限の長さの全てのビット列の集合を｛０，１｝＊と表す。例えば、ｎを自然数として、長さｎの全てのビット列の集合を｛０，１｝^{n}と表す。
【００１５】
自然数ｎに対して、｛１，・・・，ｎ｝を［ｎ］と表す。Ｓを集合として、集合Ｓから一様にｓを選択することをｓ←Ｓと表す。同一行数の行列A_1及びA_2に対して、A_1及びA_2の連結（concatenation）を
【００１６】
【数１】

$$(\mathbf{A}_1||\mathbf{A}_2)$$

と表す。行列Ａの列全体で張られる空間（つまり、行列Ａを構成する各列ベクトルを基底とする空間）をｓｐａｎ（Ａ）と表す。
【００１７】
ｉ∈｛１，２，Ｔ｝として、Z_p上の行列Ａ：＝（$a_{j,l}$）$_{j,l}$に対して、位数ｐの巡回群G_i上の行列で、その（ｊ，ｌ）成分が
【００１８】
【数２】

$$g_i^{a_{j,\ell}}$$

である行列を［Ａ］$_i$と表す。なお、この記法は、ベクトルやスカラーに対しても同様に適用する。また、（［Ａ］$_1$，［Ａ］$_2$）を［Ａ］$_{1,2}$と表す。
【００１９】

【数３】

$$\mathbf{A}^{\top}\mathbf{B}$$

が定義された行列Ａ及びＢに対して、記法の濫用ではあるが、ペアリングを

【００２０】

【数４】

$$e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{A}^{\top}\mathbf{B}]_T$$

と表す。なお、

【００２１】

【数５】

$$\top$$

は転置を表す。

【００２２】

・論理式

論理式とは、ブール変数を「かつ（ＡＮＤ）」、「または（ＯＲ）」、「否定（ＮＯＴ）」で繋いだ式である。論理式は、ファンイン２、ファンアウト１の論理回路に簡単に変換することができる。否定（ＮＯＴ）を含まない論理式を単調論理式（monotone Boolean formula）と呼び、否定（ＮＯＴ）を含む論理式を非単調論理式（non-monotone Boolean formula）と呼ぶ。本実施形態では、論理式は論理回路で表されているものとする。

【００２３】

・属性とポリシー

本実施形態では、属性の集合を以下の式（１）で定義する。

【００２４】

【数６】

$$\mathcal{X} = \bigcup_{i\in\mathbb{N}} \mathbb{Z}_p^i \times \Phi_i \qquad (1)$$

ここで、Φ$_i$は全ての単射関数φ：［ｉ］→｛０，１｝＊で構成される集合である。

【００２５】

また、ポリシーの集合を以下の式（２）で定義する。

【００２６】

【数７】

$$\mathcal{Y} = \bigcup_{i\in\mathbb{N}} \mathbb{Z}_p^i \times \mathcal{F}_i \times \Psi_i \times \mathcal{T}_i \qquad (2)$$

ここで、

【００２７】

【数８】

$\mathcal{F}_i$は入力長がiの全ての単調理論式で構成される集合

Ψ_iは全ての関数$\psi : [i] \to \{0,1\}^*$で構成される集合

$\mathcal{T}_i$は全ての関数$t : [i] \to \{0,1\}$で構成される集合

である。

【００２８】

本実施形態で説明する属性ベース暗号では、各属性は上記の式（１）で定義される集合の要素であり、各ポリシーは上記の式（２）で定義される集合の要素である。

【００２９】

また、属性

【００３０】

【数９】

$$x = (\mathbf{x} \in \mathbb{Z}_p^m, \phi)$$

がポリシー

【００３１】

【数１０】

$$y = (\mathbf{y} \in \mathbb{Z}_p^n, f, \psi, t)$$

を満たすとは、以下の式（３）で定義されるｂに対してｆ（ｂ）＝１となることを指す。すなわち、ｆ（ｂ）＝１である場合に限り復号が可能である。

【００３２】

属性ｘ及びポリシーｙに対して、ｂ＝（ｂ$_1$，・・・，ｂ$_n$）∈｛０，１｝^{n}を以下の式（３）で定義する。

【００３３】

【数１１】

$$b_i := \begin{cases} t(i) \odot \mathrm{true}(x_{\phi^{-1}(\psi(i))} = y_i) & \psi(i) \subseteq \mathrm{Im}(\phi) \\ 0 & \psi(i) \not\subseteq \mathrm{Im}(\phi) \end{cases} \quad (3)$$

ここで、

【００３４】

【数１２】

$$\odot$$

は否定排他的論理和（ＸＮＯＲ）を表し、ｔｕｒｅは真理値を表す。また、ｘ$_j$は

【００３５】
【数１３】

$$\mathbf{x} \in \mathbb{Z}_p^m$$

のｊ番目の要素であり、ｙ$_{i}$は
【００３６】
【数１４】

$$\mathbf{y} \in \mathbb{Z}_p^n$$

のｉ番目の要素である。
【００３７】
なお、上記の式（１）及び式（２）は鍵ポリシー属性ベース暗号における場合の表記であり、暗号文ポリシー属性ベース暗号では、属性の集合とポリシーの集合との定義内容が逆になる。
【００３８】
・線形秘密分散
本実施形態では線形秘密分散法を用いる。線形秘密分散法は或る関数ｆ：｛０，１｝^{n}→｛０，１｝に従って、秘密ベクトルｋを割り当てσ$_{1}$，・・・，σ$_{n}$に分散する方法である。分散された割り当てのうち、ｆ（ｂ）＝１となるようなビット列ｂのビットが１である部分に対応する割り当てを集めると元の秘密ベクトルｋを復元することができる。すなわち、ｆとｂとから簡単に計算できる集合Ｓが存在し、
【００３９】
【数１５】

$$\mathbf{k} = \sum_{i \in S} \boldsymbol{\sigma}_i$$

という単純に割り当てを足し合わせるだけで復元できる。一方で、ｆ（ｂ）＝０となるようなビット列ｂのビットが１である部分に対応する割り当てを集めてもｋを復元することができない。
【００４０】
線形秘密分散法は、以下の（Ｓ１）～（Ｓ４）に示すアルゴリズムより実現される。ここで、線形秘密分散法の入力は、単調論理式ｆ：｛０，１｝^{n}→｛０，１｝と秘密ベクトル
【００４１】

【数１６】

$$\mathbf{k} \in \mathbb{Z}_p^{\ell}$$

である。以降では、この線形秘密分散法のアルゴリズムをＳｈａｒｅとも表す。

【００４２】

（Ｓ１）論理回路で表されている単調論理式ｆの出力線（つまり、当該論理回路の出力線）にベクトルσ_{out}：＝ｋを設定する。

【００４３】

（Ｓ２）当該論理回路の各ＡＮＤゲートの入力線をａ及びｂ、出力線をｃとして、出力線ｃにベクトルσ_cが設定されている各ＡＮＤゲートについて、ベクトル

【００４４】

【数１７】

$$\mathbf{u}_g \leftarrow \mathbb{Z}_p^{\ell}$$

を選択した上で、ベクトルσ_a：＝$\sigma_c - u_g$とベクトルσ_b：＝u_gとを入力線ａと入力線ｂとにそれぞれ設定する。

【００４５】

（Ｓ３）当該論理回路の各ＯＲゲートの入力線をａ及びｂ、出力線をｃとして、出力線ｃにベクトルσ_cが設定されている各ＯＲゲートについて、ベクトルσ_a：＝σ_cとσ_b：＝σ_cとを入力線ａと入力線ｂとにそれぞれ設定する。

【００４６】

（Ｓ４）単調論理式ｆの入力線１，・・・，ｎ（つまり、当該論理回路の入力線１，・・・，ｎ）に設定されたσ_1，・・・，σ_nを秘密ベクトルｋの割り当てとして出力する。

【００４７】

なお、この線形秘密分散のアルゴリズムＳｈａｒｅは、群要素のベクトルに対しても同様に適用可能である。

【００４８】

＜本実施形態に係る属性ベース暗号＞

本実施形態に係る属性ベース暗号として、本実施形態に係る鍵ポリシー属性ベース暗号と本実施形態に係る暗号文ポリシー属性ベース暗号とについて説明する。属性ベース暗号は４つのアルゴリズム（つまり、セットアップアルゴリズムＳｅｔｕｐ、暗号化アルゴリズムＥｎｃ、鍵生成アルゴリズムＫｅｙＧｅｎ及び復号アルゴリズムＤｅｃ）で構成される。本実施形態では、素数位数ｐの巡回群G_1、G_2及びG_Tとして、双線形写像ｅ：$G_1 \times G_2 \rightarrow G_T$を持つものを用いる。これらの巡回群及び双線形写像をあわせて双線形群と呼ぶ。双線形群は既知のものを利用してもよいし、セットアップアルゴリズムＳｅｔｕｐで生成されてもよい。

【００４９】

・行列の記法

まず、属性ベース暗号の各アルゴリズムの説明と、後述する属性ベースＫＥＭ（Key Encapsulation Mechanism）の各アルゴリズムの説明とで用いる行列の記法について説明する。

【００５０】

ｋを任意の自然数として、

【００５１】

【数１８】

$$\mathcal{D}_k$$

をＺ$_p$上の（ｋ＋１）×ｋで最大階数の適当な行列の集合とする。このとき、

【００５２】

【数１９】

$$\mathbf{A} \in \mathcal{D}_k$$

に対して、Ａ*、ａ$_R$及びａ$^\perp$を次のように定義する。すなわち、或る決まった方法により行列Ａから確定的に計算されるベクトルであって、

【００５３】

【数２０】

$$\overline{\mathbf{A}} := (\mathbf{A} || \mathbf{a}_R)$$

が基底となるものをａ$_R$とする。また、

【００５４】

【数２１】

$$(\overline{\mathbf{A}}^\top)^{-1}$$

の左からｋ個の列（つまり、第１列目から第ｋ列目までの列）で構成される行列をＡ*、

【００５５】
【数２２】

$$(\overline{\mathbf{A}}^{\top})^{-1}$$

の最も右側にある列をベクトルａ$^{\perp}$とする。これらのＡ*、ａ$_{R}$及びａ$^{\perp}$には以下の関係が成り立つ。
【００５６】
【数２３】

$$\mathbf{A}^{\top}\mathbf{A}^{*}=\mathbf{I}_{k},\ \mathbf{A}^{\top}\mathbf{a}^{\perp}=\mathbf{0},\mathbf{A}^{*}\mathbf{A}^{\top}+\mathbf{a}^{\perp}\mathbf{a}_{\mathsf{R}}^{\top}=\mathbf{I}_{k+1}$$

ここで、Ｉ$_{k}$はｋ×ｋの単位行列、Ｉ$_{k+1}$は（ｋ＋１）×（ｋ＋１）の単位行列である。
【００５７】
また、行列Ｂ、ベクトルｂ$_{1}$及びベクトルｂ$_{2}$を、それぞれ、行列
【００５８】
【数２４】

$$\overline{\mathbf{B}}\in \mathsf{GL}_{k+2}(\mathbb{Z}_{p})$$

の左からｋ個の列で構成される行列、第ｋ＋１列目の列を表すベクトル及び最も右側にある列（つまり、第ｋ＋２列目の列）を表すベクトルとする。ここで、ＧＬ$_{k+2}$（Ｚ$_{p}$）は、Ｚ$_{p}$上の（ｋ＋２）×（ｋ＋２）の正則行列全体の集合（つまり、サイズｋ＋２のＺ$_{p}$上の一般線型群）である。
【００５９】
同様に、行列Ｂ*、ベクトルｂ$_{1}$*及びベクトルｂ$_{2}$*を、それぞれ、行列
【００６０】
【数２５】

$$(\overline{\mathbf{B}}^{\top})^{-1}$$

の左からｋ個の列で構成される行列、第ｋ＋１列目の列を表すベクトル及び最も右側にある列を表すベクトルとする。

【００６１】

また、簡単のため、

【００６２】

【数２６】

$$(\mathbf{b}_1||\mathbf{b}_2)$$

をＢ$_{1,2}$とも表す。この表記は他の場合（例えば、行列の場合等）にも同様に適用する。

【００６３】

・本実施形態に係る鍵ポリシー属性ベース暗号

以降では、本実施形態に係る鍵ポリシー属性ベース暗号の各アルゴリズムについて説明する。ｋを任意の自然数として、

【００６４】

【数２７】

$$H : \{0,1\}^* \to G_1^{(k+1)\times k} \times G_1^{(k+1)\times k}$$

を関数とする。また、

【００６５】

【数２８】

$$F_K : \{0,1\}^* \to \mathbb{Z}_p^{k+1} \times \mathbb{Z}_p^{k+1}$$

をＫを添字とする関数族とし、

【００６６】

【数２９】

$$\mathcal{K}$$

をＫの添字空間とする。このとき、本実施形態に係る鍵ポリシー属性ベース暗号のセットアップアルゴリズムＳｅｔｕｐ、暗号化アルゴリズムＥｎｃ、鍵生成アルゴリズムＫｅｙＧｅｎ及び復号アルゴリズムＤｅｃは、以下のように構成される。

【００６７】

Ｓｅｔｕｐ（）：セットアップアルゴリズムＳｅｔｕｐは、以下により公開鍵ｐｋとマスター秘密鍵ｍｓｋとを出力する。

【００６８】

【数３０】

$$\mathbf{A},\mathbf{B} \leftarrow \mathcal{D}_k,\ \ \mathbf{k} \leftarrow \mathbb{Z}_p^{k+1},\ \ K \leftarrow \mathcal{K},$$
$$\mathsf{pk} := (\mathbb{G}, [\mathbf{A}]_2, [\mathbf{A}^\top \mathbf{k}]_T),\ \ \mathsf{msk} := (\mathbf{A}^*, \mathbf{a}^\perp, \mathbf{B}, \mathbf{k}, K)$$

ここで、Ｇは双線形群であり、Ｇ：＝（ｐ，G_1，G_2，G_T，g_1，g_2，ｅ）である。また、g_1及びg_2はそれぞれG_1及びG_2の生成元である。上述したように、双線形群Ｇは既知のものを利用してもよいし、セットアップアルゴリズムＳｅｔｕｐで生成されてもよい。

【００６９】

Ｅｎｃ（ｐｋ，ｘ，Ｍ）：暗号化アルゴリズムＥｎｃは、公開鍵ｐｋと、属性

【００７０】

【数３１】

$$x = (\mathbf{x} \in \mathbb{Z}_p^m, \phi)$$

と、メッセージ$M \in G_T$とを入力して、以下により暗号文ct_x（属性付き暗号文ct_x）を出力する。

【００７１】

【数３２】

$$\mathbf{s} \leftarrow \mathbb{Z}_p^k,\ \ ([\mathbf{U}_{\phi(i),0}]_1, [\mathbf{U}_{\phi(i),1}]_1) := H(\phi(i)),$$
$$c_1 := [\mathbf{As}]_2,\ \ c_{2,i} := [(x_i \mathbf{U}_{\phi(i),0} + \mathbf{U}_{\phi(i),1})\mathbf{s}]_1,$$
$$c_3 := [\mathbf{s}^\top \mathbf{A}^\top \mathbf{k}]_T M \ \text{ for } i \in [m],$$
$$\mathsf{ct}_x := (x, c_1, \{c_{2,i}\}_{i\in[m]}, c_3)$$

ＫｅｙＧｅｎ（ｐｋ，ｍｓｋ，ｙ）：鍵生成アルゴリズムＫｅｙＧｅｎは、公開鍵ｐｋと、マスター秘密鍵ｍｓｋと、ポリシー

【００７２】

【数３３】

$$y = (\mathbf{y} \in \mathbb{Z}_p^n, f, \psi, t)$$

とを入力して、以下により秘密鍵ｓｋｙ（ポリシー付き秘密鍵ｓｋｙ）を出力する。

【００７３】

【数３４】

$$\mathbf{r}_1, \ldots, \mathbf{r}_d \leftarrow \mathbb{Z}_p^k,\ \ \mathbf{k}_1, \ldots, \mathbf{k}_n \leftarrow \mathsf{Share}(f, \mathbf{k}) \in \mathbb{Z}_p^{k+1},$$
$$k_{1,j} := [\mathbf{Br}_j]_2 \ \text{ for } j \in [d],$$
$$([\mathbf{U}_{\psi(i),0}]_1, [\mathbf{U}_{\psi(i),1}]_1) := H(\psi(i)),\ \ (\mathbf{u}_{\psi(i),0}, \mathbf{u}_{\psi(i),1}) := F_K(\psi(i)),$$
$$k_{2,i} := [\mathbf{k}_i + \mathbf{A}^*(y_i \mathbf{U}_{\psi(i),0}^\top + \mathbf{U}_{\psi(i),1}^\top)\mathbf{Br}_{\pi(i)} + \mathbf{a}^\perp(y_i \mathbf{u}_{\psi(i),0}^\top + \mathbf{u}_{\psi(i),1}^\top)\mathbf{Br}_{\pi(i)}]_1 \ \text{ if } t(i) = 1,$$
$$k_{2,i} := (k_{2,i,1}, k_{2,i,2}) := \begin{pmatrix} [-\mathbf{k}_i + \mathbf{A}^*\mathbf{U}_{\psi(i),0}^\top \mathbf{Br}_{\pi(i)} + \mathbf{a}^\perp \mathbf{u}_{\psi(i),0}^\top \mathbf{Br}_{\pi(i)}]_1, \\ [y_i \mathbf{k}_i + \mathbf{A}^*\mathbf{U}_{\psi(i),1}^\top \mathbf{Br}_{\pi(i)} + \mathbf{a}^\perp \mathbf{u}_{\psi(i),1}^\top \mathbf{Br}_{\pi(i)}]_1 \end{pmatrix} \ \text{ if } t(i) = 0$$
$$\text{for } i \in [n],$$
$$\mathsf{sk}_y := (y, \{k_{1,j}\}_{j\in[d]}, \{k_{2,i}\}_{i\in[n]})$$

ここで、π：［ｎ］→｛ｎ｜ｎは自然数｝はπ（ｉ）：＝｜｛ｊ｜ψ（ｊ）＝ψ（ｉ），ｊ≦ｉ｝｜となる関数であり、ｄはｆにおける同じ属性ラベルの出現回数の最大値（つまり、ｄ：＝ｍａｘ$_{ｉ∈［ｎ］}$π（ｉ））である。

【００７４】
Ｄｅｃ（ｐｋ，ｃｔ$_x$，ｓｋ$_y$）：復号アルゴリズムＤｅｃは、公開鍵ｐｋと、暗号文ｃｔ$_x$と、秘密鍵ｓｋ$_y$とを入力して、上記の式（３）によってｘ及びｙからｂを計算した上で、ｆ（ｂ）＝０である場合は復号失敗を示す⊥を出力する。一方で、ｆ（ｂ）≠０である場合は
【００７５】
【数３５】

$$\mathbf{k} = \sum_{i \in S} \mathbf{k}_i$$

を満たす集合Ｓ⊆｛ｉ｜ｂ$_i$＝１｝を計算し、以下によりＭ´を出力する。
【００７６】
【数３６】

$$D_{1,j} := e\left(\sum_{\substack{\pi(i)=j \\ i \in S_1}} k_{2,i} + \sum_{\substack{\pi(i)=j \\ i \in S_0}} \frac{1}{y_i - x_{\phi^{-1}(\psi(i))}}(x_{\phi^{-1}(\psi(i))}k_{2,i,1} + k_{2,i,2}), c_1\right),$$

$$D_{2,j} := e\left(\sum_{\substack{\pi(i)=j \\ i \in S_1}} c_{2,\phi^{-1}(\psi(i))} + \sum_{\substack{\pi(i)=j \\ i \in S_0}} \frac{1}{y_i - x_{\phi^{-1}(\psi(i))}} c_{2,\phi^{-1}(\psi(i))}, k_{1,j}\right) \quad \text{for } j \in [d],$$

$$M' := c_3 / \prod_{j \in [d]} (D_{1,j}/D_{2,j})$$

ここで、Ｓ$_1$：＝Ｓ∩｛ｉ｜ｔ（ｉ）＝１｝、Ｓ$_0$：＝Ｓ∩｛ｉ｜ｔ（ｉ）＝０｝である。
【００７７】
・本実施形態に係る暗号文ポリシー属性ベース暗号
以降では、本実施形態に係る暗号文ポリシー属性ベース暗号の各アルゴリズムについて説明する。ｋを任意の自然数として、ＧＬ$_k$（Ｚ$_p$）をサイズｋのＺ$_p$上の一般線型群、
【００７８】
【数３７】

$$H : \{0,1\}^* \to G_1^{(k+1)\times k} \times G_1^{(k+1)\times k}$$

を関数とする。また、

【００７９】

【数３８】

$$F_K : \{0,1\}^* \to \mathbb{Z}_p^{k+2} \times \mathbb{Z}_p^{k+2}$$

をＫを添字とする関数族とし、

【００８０】

【数３９】

$$\mathcal{K}$$

をＫの添字空間とする。このとき、本実施形態に係る暗号文ポリシー属性ベース暗号のセットアップアルゴリズムＳｅｔｕｐ、暗号化アルゴリズムＥｎｃ、鍵生成アルゴリズムＫｅｙＧｅｎ及び復号アルゴリズムＤｅｃは、以下のように構成される。

【００８１】

Ｓｅｔｕｐ（）：セットアップアルゴリズムＳｅｔｕｐは、以下により公開鍵ｐｋとマスター秘密鍵ｍｓｋとを出力する。

【００８２】

【数４０】

$$\begin{aligned}
&\mathbf{A} \leftarrow \mathcal{D}_k,\ \ \overline{\mathbf{B}} \leftarrow \mathsf{GL}_{k+2}(\mathbb{Z}_p),\ \ \mathbf{W} \leftarrow \mathbb{Z}_p^{(k+1)\times(k+2)},\\
&\mathbf{k} \leftarrow \mathbb{Z}_p^{k+2},\ \ K \leftarrow \mathcal{K},\\
&\mathsf{pk} := (\mathbb{G}, [\mathbf{B}]_2, [\mathbf{WB}]_1, [\mathbf{B}^\top \mathbf{k}]_T),\\
&\mathsf{msk} := (\mathbf{A}, \mathbf{W}^\top \mathbf{A}, \mathbf{B}^*, \mathbf{B}^*_{12}, \mathbf{k}, K)
\end{aligned}$$

ここで、Ｇは双線形群であり、Ｇ：＝（ｐ，Ｇ１，Ｇ２，Ｇ Ｔ，ｇ１，ｇ２，ｅ）である。上述したように、双線形群Ｇは既知のものを利用してもよいし、セットアップアルゴリズムＳｅｔｕｐで生成されてもよい。

【００８３】

Ｅｎｃ（ｐｋ，ｘ，Ｍ）：暗号化アルゴリズムＥｎｃは、公開鍵ｐｋと、ポリシー

【００８４】

【数４１】

$$x = (\mathbf{x} \in \mathbb{Z}_p^n, f, \psi, t)$$

と、メッセージＭ∈Ｇ Ｔとを入力して、以下により暗号文ｃｔ ｘ（ポリシー付き暗号文ｃｔ ｘ）を出力する。

【００８５】

【数４２】

$$\begin{aligned}
&\mathbf{r}, \mathbf{r}_1, \ldots, \mathbf{r}_d \leftarrow \mathbb{Z}_p^k, \ [\mathbf{w}_1]_1, \ldots, [\mathbf{w}_n]_1 \leftarrow \mathsf{Share}(f, [\mathbf{WBr}]_1) \in \mathbb{Z}_p^{k+1}, \\
&c_1 := [\mathbf{Br}]_2, \ c_{2,j} := [\mathbf{Br}_j]_2 \ \text{ for } j \in [d], \ c_4 := [\mathbf{r}^\top \mathbf{B}^\top \mathbf{k}]_T M, \\
&([\mathbf{U}_{\psi(i),0}]_1, [\mathbf{U}_{\psi(i),1}]_1) := H(\psi(i)), \\
&c_{3,i} := [\mathbf{w}_i + (x_i \mathbf{U}_{\psi(i),0} + \mathbf{U}_{\psi(i),1}) \mathbf{r}_{\pi(i)}]_1 \ \text{ if } t(i) = 1, \\
&c_{3,i} := (c_{3,i,1}, c_{3,i,2}) := ([-\mathbf{w}_i + \mathbf{U}_{\psi(i),0} \mathbf{r}_{\pi(i)}]_1, [x_i \mathbf{w}_i + \mathbf{U}_{\psi(i),1} \mathbf{r}_{\pi(i)}]_1) \ \text{ if } t(i) = 0 \\
&\text{for } i \in [n], \\
&\mathbf{ct}_x := (x, c_1, \{c_{2,j}\}_{j \in [d]}, \{c_{3,i}\}_{i \in [n]}, c_4)
\end{aligned}$$

ここで、π：［ｎ］→｛ｎ｜ｎは自然数｝はπ（ｉ）：＝｜｛ｊ｜ψ（ｊ）＝ψ（ｉ），ｊ≦ｉ｝｜となる関数であり、ｄはｆにおける同じ属性ラベルの出現回数の最大値（つまり、ｄ：＝ｍａｘ ｉ∈［ｎ］ π（ｉ））である。

【００８６】

ＫｅｙＧｅｎ（ｐｋ，ｍｓｋ，ｙ）：鍵生成アルゴリズムＫｅｙＧｅｎは、公開鍵ｐｋと、マスター秘密鍵ｍｓｋと、属性

【００８７】

【数４３】

$$y = (\mathbf{y} \in \mathbb{Z}_p^m, \phi)$$

とを入力して、以下により秘密鍵ｓｋｙ（属性付き秘密鍵ｓｋｙ）を出力する。

【００８８】

【数４４】

$$\mathbf{s} \leftarrow \mathbb{Z}_p^k,\ \ ([\mathbf{U}_{\phi(i),0}]_1, [\mathbf{U}_{\phi(i),1}]_1) := H(\phi(i)),\ \ (\mathbf{V}_{\phi(i),0}, \mathbf{V}_{\phi(i),1}) := F_K(\phi(i))$$
$$k_1 := [\mathbf{As}]_2,\ \ k_2 := [\mathbf{k} + \mathbf{W}^\top \mathbf{As}]_1,$$
$$k_{3,i} := [\mathbf{B}^*(y_i \mathbf{U}_{\phi(i),0}^\top + \mathbf{U}_{\phi(i),1}^\top)\mathbf{As} + \mathbf{B}_{12}^*(y_i \mathbf{V}_{\phi(i),0}^\top + \mathbf{V}_{\phi(i),1}^\top)\mathbf{As}]_1 \ \text{ for } i \in [m],$$
$$\mathsf{sk}_y := (y, k_1, k_2, \{k_{3,i}\}_{i \in [m]})$$

Ｄｅｃ（ｐｋ，ｃｔ$_x$，ｓｋ$_y$）：復号アルゴリズムＤｅｃは、公開鍵ｐｋと、暗号文ｃｔ$_x$と、秘密鍵ｓｋ$_y$とを入力して、上記の式（３）によってｘ及びｙからｂを計算した上で、ｆ（ｂ）＝０である場合は復号失敗を示す⊥を出力する。一方で、ｆ（ｂ）≠０である場合は

【００８９】

【数４５】

$$\mathbf{WBr} = \sum_{i \in S} \mathbf{w}_i$$

を満たす集合Ｓ⊆｛ｉ｜ｂ$_i$＝１｝を計算し、以下によりＭ´を出力する。

【００９０】

【数４６】

$$D_{1,j} := e\left(\sum_{\substack{\pi(i)=j \\ i\in S_1}} c_{3,i} + \sum_{\substack{\pi(i)=j \\ i\in S_0}} \frac{1}{x_i - y_{\phi^{-1}(\psi(i))}}(y_{\phi^{-1}(\psi(i))}c_{3,i,1} + c_{3,i,2}), k_1\right),$$

$$D_{2,j} := e\left(\sum_{\substack{\pi(i)=j \\ i\in S_1}} k_{3,\phi^{-1}(\psi(i))} + \sum_{\substack{\pi(i)=j \\ i\in S_0}} \frac{1}{x_i - y_{\phi^{-1}(\psi(i))}} k_{3,\phi^{-1}(\psi(i))}, c_{2,j}\right) \quad \text{for } j \in [d],$$

$$M' := c_4 / \left(e(k_2, c_1) / \prod_{j\in[d]} (D_{1,j}/D_{2,j})\right)$$

ここで、$S_1 := S \cap \{i \mid t(i) = 1\}$、$S_0 := S \cap \{i \mid t(i) = 0\}$である。

【００９１】

＜本実施形態に係る属性ベースＫＥＭ＞

上述した本実施形態に係る鍵ポリシー属性ベース暗号及び暗号文ポリシー属性ベース暗号は、ＫＥＭ方式にも応用可能である。一般的に公開鍵暗号技術は動作が遅いため、大容量のデータを暗号化する場合は、公開鍵暗号で共通鍵暗号に用いる秘密鍵を安全に配送し、データの方は共通鍵暗号で暗号化することが多い。共通鍵暗号の秘密鍵（以降、「共通鍵」とも表す。）を安全に配送するために用いられる方式がＫＥＭと呼ばれる。

【００９２】

そこで、本実施形態に係る鍵ポリシー属性ベース暗号をＫＥＭに応用した鍵ポリシー属性ベースＫＥＭと、本実施形態に係る暗号文ポリシー属性ベース暗号をＫＥＭに応用した暗号文ポリシー属性ベースＫＥＭとについて説明する。

【００９３】

・本実施形態に係る鍵ポリシー属性ベースＫＥＭ

以降では、本実施形態に係る鍵ポリシー属性ベースＫＥＭの各アルゴリズムについて説明する。関数Ｈ及び関数族F_Kは、上記で説明した「本実施形態に係る鍵ポリシー属性ベース暗号」と同様として、

【００９４】

【数４７】

$$H_2 : G_T \to \mathcal{L}$$

を関数とする。ここで、

【００９５】

【数４８】

$$\mathcal{L}$$

は共通鍵暗号の秘密鍵空間である。このとき、本実施形態に係る鍵ポリシー属性ベースＫＥＭのセットアップアルゴリズムＳｅｔｕｐ、暗号化アルゴリズムＥｎｃ、鍵生成アルゴリズムＫｅｙＧｅｎ及び復号アルゴリズムＤｅｃは、以下のように構成される。

【００９６】

Ｓｅｔｕｐ（）：セットアップアルゴリズムＳｅｔｕｐは、以下により公開鍵ｐｋとマスター秘密鍵ｍｓｋとを出力する。

【００９７】

【数４９】

$$\mathbf{A},\mathbf{B} \leftarrow \mathcal{D}_k,\ \ \mathbf{k} \leftarrow \mathbb{Z}_p^{k+1},\ \ K \leftarrow \mathcal{K},$$
$$\mathsf{pk} := (\mathbb{G}, [\mathbf{A}]_2, [\mathbf{A}^\top \mathbf{k}]_T),\ \ \mathsf{msk} := (\mathbf{A}^*, \mathbf{a}^\perp, \mathbf{B}, \mathbf{k}, K)$$

ここで、Ｇは双線形群であり、Ｇ：＝（ｐ，G_1，G_2，G_T，g_1，g_2，ｅ）である。上述したように、双線形群Ｇは既知のものを利用してもよいし、セットアップアルゴリズムＳｅｔｕｐで生成されてもよい。

【００９８】

Ｅｎｃ（ｐｋ，ｘ）：暗号化アルゴリズムＥｎｃは、公開鍵ｐｋと、属性

【００９９】

【数５０】

$$x = (\mathbf{x} \in \mathbb{Z}_p^m, \phi)$$

とを入力して、以下により暗号文ct_x（属性付き暗号文ct_x）と、共通鍵Ｌとを出力する。

【０１００】

【数５１】

$$\mathbf{s} \leftarrow \mathbb{Z}_p^k,\ \ ([\mathbf{U}_{\phi(i),0}]_1, [\mathbf{U}_{\phi(i),1}]_1) := H(\phi(i)),$$
$$c_1 := [\mathbf{As}]_2,\ \ c_{2,i} := [(x_i \mathbf{U}_{\phi(i),0} + \mathbf{U}_{\phi(i),1})\mathbf{s}]_1,$$
$$L := H_2([\mathbf{s}^\top \mathbf{A}^\top \mathbf{k}]_T)\ \text{ for } i \in [m],$$
$$\mathbf{ct}_x := (x, c_1, \{c_{2,i}\}_{i\in[m]})$$

ＫｅｙＧｅｎ（ｐｋ，ｍｓｋ，ｙ）：鍵生成アルゴリズムＫｅｙＧｅｎは、公開鍵ｐｋと、マスター秘密鍵ｍｓｋと、ポリシー

【０１０１】

【数５２】

$$y = (\mathbf{y} \in \mathbb{Z}_p^n, f, \psi, t)$$

とを入力して、以下により秘密鍵ｓｋｙ（ポリシー付き秘密鍵ｓｋｙ）を出力する。

【０１０２】

【数５３】

$$\mathbf{r}_1, \ldots, \mathbf{r}_d \leftarrow \mathbb{Z}_p^k,\ \ \mathbf{k}_1, \ldots, \mathbf{k}_n \leftarrow \mathsf{Share}(f, \mathbf{k}) \in \mathbb{Z}_p^{k+1},$$
$$k_{1,j} := [\mathbf{Br}_j]_2\ \text{ for } j \in [d],$$
$$([\mathbf{U}_{\psi(i),0}]_1, [\mathbf{U}_{\psi(i),1}]_1) := H(\psi(i)),\ \ (\mathbf{u}_{\psi(i),0}, \mathbf{u}_{\psi(i),1}) := F_K(\psi(i)),$$
$$k_{2,i} := [\mathbf{k}_i + \mathbf{A}^*(y_i \mathbf{U}_{\psi(i),0}^\top + \mathbf{U}_{\psi(i),1}^\top)\mathbf{Br}_{\pi(i)} + \mathbf{a}^\perp(y_i \mathbf{u}_{\psi(i),0}^\top + \mathbf{u}_{\psi(i),1}^\top)\mathbf{Br}_{\pi(i)}]_1\ \text{ if } t(i) = 1,$$
$$k_{2,i} := (k_{2,i,1}, k_{2,i,2}) := \begin{pmatrix} [-\mathbf{k}_i + \mathbf{A}^*\mathbf{U}_{\psi(i),0}^\top \mathbf{Br}_{\pi(i)} + \mathbf{a}^\perp \mathbf{u}_{\psi(i),0}^\top \mathbf{Br}_{\pi(i)}]_1, \\ [y_i \mathbf{k}_i + \mathbf{A}^*\mathbf{U}_{\psi(i),1}^\top \mathbf{Br}_{\pi(i)} + \mathbf{a}^\perp \mathbf{u}_{\psi(i),1}^\top \mathbf{Br}_{\pi(i)}]_1 \end{pmatrix}\ \text{ if } t(i) = 0$$
$$\text{for } i \in [n],$$
$$\mathsf{sk}_y := (y, \{k_{1,j}\}_{j\in[d]}, \{k_{2,i}\}_{i\in[n]})$$

ここで、π：［ｎ］→｛ｎ｜ｎは自然数｝はπ（ｉ）：＝｜｛ｊ｜ψ（ｊ）＝ψ（ｉ），ｊ≦ｉ｝｜となる関数であり、ｄはｆにおける同じ属性ラベルの出現回数の最大値（つまり、ｄ：＝ｍａｘ$_{ｉ∈［ｎ］}$π（ｉ））である。

【０１０３】
Ｄｅｃ（ｐｋ，ｃｔ$_x$，ｓｋ$_y$）：復号アルゴリズムＤｅｃは、公開鍵ｐｋと、暗号文ｃｔ$_x$と、秘密鍵ｓｋ$_y$とを入力して、上記の式（３）によってｘ及びｙからｂを計算した上で、ｆ（ｂ）＝０である場合は復号失敗を示す⊥を出力する。一方で、ｆ（ｂ）≠０である場合は
【０１０４】
【数５４】

$$\mathbf{k} = \sum_{i \in S} \mathbf{k}_i$$

を満たす集合Ｓ⊆｛ｉ｜ｂ$_i$＝１｝を計算し、以下により共通鍵Ｌ´を出力する。
【０１０５】
【数５５】

$$D_{1,j} := e\left(\sum_{\substack{\pi(i)=j \\ i \in S_1}} k_{2,i} + \sum_{\substack{\pi(i)=j \\ i \in S_0}} \frac{1}{y_i - x_{\phi^{-1}(\psi(i))}} (x_{\phi^{-1}(\psi(i))} k_{2,i,1} + k_{2,i,2}), c_1 \right),$$

$$D_{2,j} := e\left(\sum_{\substack{\pi(i)=j \\ i \in S_1}} c_{2,\phi^{-1}(\psi(i))} + \sum_{\substack{\pi(i)=j \\ i \in S_0}} \frac{1}{y_i - x_{\phi^{-1}(\psi(i))}} c_{2,\phi^{-1}(\psi(i))}, k_{1,j} \right) \quad \text{for } j \in [d],$$

$$L' := H_2\left(\prod_{j \in [d]} (D_{1,j} / D_{2,j}) \right)$$

ここで、Ｓ$_1$：＝Ｓ∩｛ｉ｜ｔ（ｉ）＝１｝、Ｓ$_0$：＝Ｓ∩｛ｉ｜ｔ（ｉ）＝０｝である。
【０１０６】
・本実施形態に係る暗号文ポリシー属性ベースＫＥＭ
以降では、本実施形態に係る暗号文ポリシー属性ベースＫＥＭの各アルゴリズムについて説明する。関数Ｈ及び関数族Ｆ$_K$は、上記で説明した「本実施形態に係る暗号文ポリシー属性ベース暗号」と同様として、
【０１０７】
【数５６】

$$H_2 : G_T \to \mathcal{L}$$

を関数とする。ここで、
【０１０８】
【数５７】

$$\mathcal{L}$$

は共通鍵暗号の秘密鍵空間である。このとき、本実施形態に係る暗号文ポリシー属性ベースＫＥＭのセットアップアルゴリズムＳｅｔｕｐ、暗号化アルゴリズムＥｎｃ、鍵生成アルゴリズムＫｅｙＧｅｎ及び復号アルゴリズムＤｅｃは、以下のように構成される。
【０１０９】
Ｓｅｔｕｐ（）：セットアップアルゴリズムＳｅｔｕｐは、以下により公開鍵ｐｋとマスター秘密鍵ｍｓｋとを出力する。
【０１１０】
【数５８】

$$\overline{\mathbf{B}} \leftarrow \mathsf{GL}_{k+2}(\mathbb{Z}_p),\ \ \mathbf{W} \leftarrow \mathbb{Z}_p^{(k+1)\times(k+2)},\ \ \mathbf{k} \leftarrow \mathbb{Z}_p^{k+2},\ \ K \leftarrow \mathcal{K},$$
$$\mathsf{pk} := (\mathbb{G}, [\mathbf{B}]_2, [\mathbf{WB}]_1, [\mathbf{B}^\top \mathbf{k}]_T),$$
$$\mathsf{msk} := (\mathbf{A}, \mathbf{W}^\top \mathbf{A}, \mathbf{B}^*, \mathbf{B}^*_{12}, \mathbf{k}, K)$$

ここで、Ｇは双線形群であり、Ｇ：＝（ｐ，Ｇ１，Ｇ２，ＧＴ，ｇ１，ｇ２，ｅ）である。上述したように、双線形群Ｇは既知のものを利用してもよいし、セットアップアルゴリズムＳｅｔｕｐで生成されてもよい。
【０１１１】
Ｅｎｃ（ｐｋ，ｘ）：暗号化アルゴリズムＥｎｃは、公開鍵ｐｋと、ポリシー
【０１１２】
【数５９】

$$x = (\mathbf{x} \in \mathbb{Z}_p^n, f, \psi, t)$$

とを入力して、以下により暗号文ｃｔ$_x$（ポリシー付き暗号文ｃｔ$_x$）と、共通鍵Ｌとを出力する。

【０１１３】

【数６０】

$$\begin{aligned}
&\mathbf{r}, \mathbf{r}_1, \ldots, \mathbf{r}_d \leftarrow \mathbb{Z}_p^k, \ [\mathbf{w}_1]_1, \ldots, [\mathbf{w}_n]_1 \leftarrow \mathsf{Share}(f, [\mathbf{WBr}]_1) \in \mathbb{Z}_p^{k+1}, \\
&c_1 := [\mathbf{Br}]_2, \ c_{2,j} := [\mathbf{Br}_j]_2 \ \text{ for } j \in [d], \ L := H_2([\mathbf{r}^\top \mathbf{B}^\top \mathbf{k}]_T), \\
&([\mathbf{U}_{\psi(i),0}]_1, [\mathbf{U}_{\psi(i),1}]_1) := H(\psi(i)), \\
&c_{3,i} := [\mathbf{w}_i + (x_i \mathbf{U}_{\psi(i),0} + \mathbf{U}_{\psi(i),1}) \mathbf{r}_{\pi(i)}]_1 \ \text{ if } t(i) = 1, \\
&c_{3,i} := (c_{3,i,1}, c_{3,i,2}) := ([-\mathbf{w}_i + \mathbf{U}_{\psi(i),0} \mathbf{r}_{\pi(i)}]_1, [x_i \mathbf{w}_i + \mathbf{U}_{\psi(i),1} \mathbf{r}_{\pi(i)}]_1) \ \text{ if } t(i) = 0 \\
&\text{for } i \in [n], \\
&\mathrm{ct}_x := (x, c_1, \{c_{2,j}\}_{j \in [d]}, \{c_{3,i}\}_{i \in [n]})
\end{aligned}$$

ここで、π：［ｎ］→｛ｎ｜ｎは自然数｝はπ（ｉ）：＝｜｛ｊ｜ψ（ｊ）＝ψ（ｉ），ｊ≦ｉ｝｜となる関数であり、ｄはｆにおける同じ属性ラベルの出現回数の最大値（つまり、ｄ：＝ｍａｘ$_{ｉ∈［ｎ］}$π（ｉ））である。

【０１１４】

ＫｅｙＧｅｎ（ｐｋ，ｍｓｋ，ｙ）：鍵生成アルゴリズムＫｅｙＧｅｎは、公開鍵ｐｋと、マスター秘密鍵ｍｓｋと、属性

【０１１５】

【数６１】

$$y = (\mathbf{y} \in \mathbb{Z}_p^m, \phi)$$

とを入力して、以下により秘密鍵ｓｋ$_y$（属性付き秘密鍵ｓｋ$_y$）を出力する。

【０１１６】

【数６２】

$$\mathbf{s} \leftarrow \mathbb{Z}_p^k,\ \ ([\mathbf{U}_{\phi(i),0}]_1, [\mathbf{U}_{\phi(i),1}]_1) := H(\phi(i)),\ \ (\mathbf{V}_{\phi(i),0}, \mathbf{V}_{\phi(i),1}) := F_K(\phi(i))$$
$$k_1 := [\mathbf{As}]_2,\ \ k_2 := [\mathbf{k} + \mathbf{W}^\top \mathbf{As}]_1,$$
$$k_{3,i} := [\mathbf{B}^*(y_i \mathbf{U}_{\phi(i),0}^\top + \mathbf{U}_{\phi(i),1}^\top)\mathbf{As} + \mathbf{B}_{12}^*(y_i \mathbf{V}_{\phi(i),0}^\top + \mathbf{V}_{\phi(i),1}^\top)\mathbf{As}]_1 \ \text{ for } i \in [m],$$
$$\mathsf{sk}_y := (y, k_1, k_2, \{k_{3,i}\}_{i\in[m]}).$$

Ｄｅｃ（ｐｋ，ｃｔ$_x$，ｓｋ$_y$）：復号アルゴリズムＤｅｃは、公開鍵ｐｋと、暗号文ｃｔ$_x$と、秘密鍵ｓｋ$_y$とを入力して、上記の式（３）によってｘ及びｙからｂを計算した上で、ｆ（ｂ）＝０である場合は復号失敗を示す⊥を出力する。一方で、ｆ（ｂ）≠０である場合は

【０１１７】

【数６３】

$$\mathbf{WBr} = \sum_{i\in S} \mathbf{w}_i$$

を満たす集合Ｓ⊆｛ｉ｜ｂ$_i$＝１｝を計算し、以下により共通鍵Ｌ′を出力する。

【０１１８】

【数６４】

$$D_{1,j} := e\left(\sum_{\substack{\pi(i)=j \\ i\in S_1}} c_{3,i} + \sum_{\substack{\pi(i)=j \\ i\in S_0}} \frac{1}{x_i - y_{\phi^{-1}(\psi(i))}}(y_{\phi^{-1}(\psi(i))} c_{3,i,1} + c_{3,i,2}), k_1\right),$$
$$D_{2,j} := e\left(\sum_{\substack{\pi(i)=j \\ i\in S_1}} k_{3,\phi^{-1}(\psi(i))} + \sum_{\substack{\pi(i)=j \\ i\in S_0}} \frac{1}{x_i - y_{\phi^{-1}(\psi(i))}} k_{3,\phi^{-1}(\psi(i))}, c_{2,j}\right) \ \text{ for } j \in [d],$$
$$L' := H_2\left(e(k_2, c_1) / \prod_{j\in[d]} (D_{1,j}/D_{2,j})\right)$$

ここで、Ｓ$_1$：＝Ｓ∩｛ｉ｜ｔ（ｉ）＝１｝、Ｓ$_0$：＝Ｓ∩｛ｉ｜ｔ（ｉ）＝０｝であ

る。

【０１１９】

＜暗号システム１の全体構成＞

次に、上記で説明した「本実施形態に係る鍵ポリシー属性ベース暗号」、「本実施形態に係る暗号文ポリシー属性ベース暗号」、「本実施形態に係る鍵ポリシー属性ベースＫＥＭ」及び「本実施形態に係る暗号文ポリシー属性ベースＫＥＭ」を実現する暗号システム１の全体構成について、図１を参照しながら説明する。図１は、本実施形態に係る暗号システム１の全体構成の一例を示す図である。

【０１２０】

図１に示すように、本実施形態に係る暗号システム１には、鍵生成装置１０と、暗号化装置２０と、復号装置３０とが含まれる。これらの各装置は、例えばインターネット等の通信ネットワークＮを介して通信可能に接続される。なお、図１に示す例では、暗号化装置２０及び復号装置３０がそれぞれ１台ずつである場合を示しているが、これらの装置はそれぞれ複数台存在してもよい。また、鍵生成装置１０も複数台存在してもよい。

【０１２１】

鍵生成装置１０は、セットアップアルゴリズムＳｅｔｕｐや鍵生成アルゴリズムＫｅｙＧｅｎを実行して鍵を生成するコンピュータ又はコンピュータシステムである。ここで、鍵生成装置１０は、セットアップ処理部１０１と、鍵生成処理部１０２と、記憶部１０３とを有する。なお、セットアップ処理部１０１及び鍵生成処理部１０２は、鍵生成装置１０にインストールされた１以上のプログラムがプロセッサ等に実行させる処理により実現される。また、記憶部１０３は、例えば、補助記憶装置等の各種メモリを用いて実現可能である。

【０１２２】

セットアップ処理部１０１は、セットアップアルゴリズムＳｅｔｕｐを実行する。鍵生成処理部１０２は、鍵生成アルゴリズムＫｅｙＧｅｎを実行する。記憶部１０３には、各種データ（例えば、セットアップアルゴリズムＳｅｔｕｐで出力された公開鍵ｐｋやマスター秘密鍵ｍｓｋ等）が記憶される。

【０１２３】

暗号化装置２０は、暗号化アルゴリズムＥｎｃを実行して暗号文を生成するコンピュータ又はコンピュータシステムである。ここで、暗号化装置２０は、暗号化処理部２０１と、記憶部２０２とを有する。暗号化処理部２０１は、暗号化装置２０にインストールされた１以上のプログラムがプロセッサ等に実行させる処理により実現される。また、記憶部２０２は、例えば、補助記憶装置等の各種メモリを用いて実現可能である。

【０１２４】

暗号化処理部２０１は、暗号化アルゴリズムＥｎｃを実行する。記憶部２０２には、各種データ（例えば、暗号化アルゴリズムＥｎｃに入力されるデータ等）が記憶される。

【０１２５】

復号装置３０は、復号アルゴリズムＤｅｃを実行して暗号文を復号するコンピュータ又はコンピュータシステムである。ここで、復号装置３０は、復号処理部３０１と、記憶部３０２とを有する。復号処理部３０１は、復号装置３０にインストールされた１以上のプログラムがプロセッサ等に実行させる処理により実現される。また、記憶部３０２は、例えば、補助記憶装置等の各種メモリを用いて実現可能である。

【０１２６】

復号処理部３０１は、復号アルゴリズムＤｅｃを実行する。記憶部３０２には、各種データ（例えば、復号アルゴリズムＤｅｃに入力されるデータや復号アルゴリズムＤｅｃにより出力されるデータ等）が記憶される。

【０１２７】

なお、図１に示す暗号システム１の構成は一例であって、他の構成であってもよい。例えば、暗号化装置２０と復号装置３０とが同一の装置で実現されていてもよい。この場合、当該装置は、例えば、暗号化処理部２０１と、復号処理部３０１と、記憶部とを有する

ことなる。

【０１２８】

＜暗号システム１が実行する処理の流れ＞

以降では、本実施形態に係る暗号システム１が実行する処理の流れについて説明する。

【０１２９】

・本実施形態に係る鍵ポリシー属性ベース暗号

本実施形態に係る暗号システム１が「本実施形態に係る鍵ポリシー属性ベース暗号」を実現する場合には、以下のＳｔｅｐ１－１～Ｓｔｅｐ１－４が実行される。

【０１３０】

Ｓｔｅｐ１－１）鍵生成装置１０のセットアップ処理部１０１は、本実施形態に係る鍵ポリシー属性ベース暗号のセットアップアルゴリズムＳｅｔｕｐを実行する。これにより、公開鍵ｐｋとマスター秘密鍵ｍｓｋとが生成及び出力される。これらの公開鍵ｐｋ及びマスター秘密鍵ｍｓｋは記憶部１０３に記憶される。また、公開鍵ｐｋは公開される。

【０１３１】

Ｓｔｅｐ１－２）暗号化装置２０の暗号化処理部２０１は、公開鍵ｐｋと属性ｘとメッセージＭとを入力として、本実施形態に係る鍵ポリシー属性ベース暗号の暗号化アルゴリズムＥｎｃを実行する。これにより、属性付き暗号文ct_xが出力される。属性付き暗号文ct_xは、例えば、通信ネットワークＮを介して復号装置３０に送信される。属性付き暗号文ct_xは記憶部２０２に記憶されてもよい。

【０１３２】

Ｓｔｅｐ１－３）鍵生成装置１０の鍵生成処理部１０２は、公開鍵ｐｋとマスター秘密鍵ｍｓｋとポリシーｙとを入力として、本実施形態に係る鍵ポリシー属性ベース暗号の鍵生成アルゴリズムＫｅｙＧｅｎを実行する。これにより、ポリシー付き秘密鍵sk_yが生成される。ポリシー付き秘密鍵sk_yは、例えば、通信ネットワークＮを介して復号装置３０に送信される。

【０１３３】

Ｓｔｅｐ１－４）復号装置３０の復号処理部３０１は、公開鍵ｐｋと属性付き暗号文ct_xとポリシー付き秘密鍵sk_yとを入力として、本実施形態に係る鍵ポリシー属性ベース暗号の復号アルゴリズムＤｅｃを実行する。これにより、復号失敗を示す⊥又はメッセージＭ´のいずれかが出力される。この出力結果は、例えば、記憶部３０２に記憶される。

【０１３４】

・本実施形態に係る暗号文ポリシー属性ベース暗号

本実施形態に係る暗号システム１が「本実施形態に係る暗号文ポリシー属性ベース暗号」を実現する場合には、以下のＳｔｅｐ２－１～Ｓｔｅｐ２－４が実行される。

【０１３５】

Ｓｔｅｐ２－１）鍵生成装置１０のセットアップ処理部１０１は、本実施形態に係る暗号文ポリシー属性ベース暗号のセットアップアルゴリズムＳｅｔｕｐを実行する。これにより、公開鍵ｐｋとマスター秘密鍵ｍｓｋとが生成及び出力される。これらの公開鍵ｐｋ及びマスター秘密鍵ｍｓｋは記憶部１０３に記憶される。また、公開鍵ｐｋは公開される。

【０１３６】

Ｓｔｅｐ２－２）暗号化装置２０の暗号化処理部２０１は、公開鍵ｐｋとポリシーｘとメッセージＭとを入力として、本実施形態に係る暗号文ポリシー属性ベース暗号の暗号化アルゴリズムＥｎｃを実行する。これにより、ポリシー付き暗号文ct_xが出力される。ポリシー付き暗号文ct_xは、例えば、通信ネットワークＮを介して復号装置３０に送信される。ポリシー付き暗号文ct_xは記憶部２０２に記憶されてもよい。

【０１３７】

Ｓｔｅｐ２－３）鍵生成装置１０の鍵生成処理部１０２は、公開鍵ｐｋとマスター秘密鍵ｍｓｋと属性ｙとを入力として、本実施形態に係る暗号文ポリシー属性ベース暗号の鍵生成アルゴリズムＫｅｙＧｅｎを実行する。これにより、属性付き秘密鍵sk_yが生成される。属性付き秘密鍵sk_yは、例えば、通信ネットワークＮを介して復号装置３０に送

信される。
【０１３８】
　Ｓｔｅｐ２－４）復号装置３０の復号処理部３０１は、公開鍵ｐｋとポリシー付き暗号文ct_xと属性付き秘密鍵sk_yとを入力として、本実施形態に係る暗号文ポリシー属性ベース暗号の復号アルゴリズムＤｅｃを実行する。これにより、復号失敗を示す⊥又はメッセージＭ´のいずれかが出力される。この出力結果は、例えば、記憶部３０２に記憶される。
【０１３９】
　・本実施形態に係る鍵ポリシー属性ベースＫＥＭ
　本実施形態に係る暗号システム１が「本実施形態に係る鍵ポリシー属性ベースＫＥＭ」を実現する場合には、以下のＳｔｅｐ３－１～Ｓｔｅｐ３－４が実行される。
【０１４０】
　Ｓｔｅｐ３－１）鍵生成装置１０のセットアップ処理部１０１は、本実施形態に係る鍵ポリシー属性ベースＫＥＭのセットアップアルゴリズムＳｅｔｕｐを実行する。これにより、公開鍵ｐｋとマスター秘密鍵ｍｓｋとが生成及び出力される。これらの公開鍵ｐｋ及びマスター秘密鍵ｍｓｋは記憶部１０３に記憶される。また、公開鍵ｐｋは公開される。
【０１４１】
　Ｓｔｅｐ３－２）暗号化装置２０の暗号化処理部２０１は、公開鍵ｐｋと属性ｘとを入力として、本実施形態に係る鍵ポリシー属性ベースＫＥＭの暗号化アルゴリズムＥｎｃを実行する。これにより、属性付き暗号文ct_xと共通鍵Ｌとが出力される。属性付き暗号文ct_xは、例えば、通信ネットワークＮを介して復号装置３０に送信される。属性付き暗号文ct_xは記憶部２０２に記憶されてもよい。また、共通鍵Ｌは記憶部２０２に記憶される。
【０１４２】
　Ｓｔｅｐ３－３）鍵生成装置１０の鍵生成処理部１０２は、公開鍵ｐｋとマスター秘密鍵ｍｓｋとポリシーｙとを入力として、本実施形態に係る鍵ポリシー属性ベースＫＥＭの鍵生成アルゴリズムＫｅｙＧｅｎを実行する。これにより、ポリシー付き秘密鍵sk_yが生成される。ポリシー付き秘密鍵sk_yは、例えば、通信ネットワークＮを介して復号装置３０に送信される。
【０１４３】
　Ｓｔｅｐ３－４）復号装置３０の復号処理部３０１は、公開鍵ｐｋと属性付き暗号文ct_xとポリシー付き秘密鍵sk_yとを入力として、本実施形態に係る鍵ポリシー属性ベースＫＥＭの復号アルゴリズムＤｅｃを実行する。これにより、復号失敗を示す⊥又は共通鍵Ｋ´のいずれかが出力される。この出力結果は、例えば、記憶部３０２に記憶される。
【０１４４】
　・本実施形態に係る暗号文ポリシー属性ベースＫＥＭ
　本実施形態に係る暗号システム１が「本実施形態に係る暗号文ポリシー属性ベースＫＥＭ」を実現する場合には、以下のＳｔｅｐ４－１～Ｓｔｅｐ４－４が実行される。
【０１４５】
　Ｓｔｅｐ４－１）鍵生成装置１０のセットアップ処理部１０１は、本実施形態に係る暗号文ポリシー属性ベースＫＥＭのセットアップアルゴリズムＳｅｔｕｐを実行する。これにより、公開鍵ｐｋとマスター秘密鍵ｍｓｋとが生成及び出力される。これらの公開鍵ｐｋ及びマスター秘密鍵ｍｓｋは記憶部１０３に記憶される。また、公開鍵ｐｋは公開される。
【０１４６】
　Ｓｔｅｐ４－２）暗号化装置２０の暗号化処理部２０１は、公開鍵ｐｋとポリシーｘとを入力として、本実施形態に係る暗号文ポリシー属性ベースＫＥＭの暗号化アルゴリズムＥｎｃを実行する。これにより、ポリシー付き暗号文ct_xと共通鍵Ｌとが出力される。ポリシー付き暗号文ct_xは、例えば、通信ネットワークＮを介して復号装置３０に送信される。ポリシー付き暗号文ct_xは記憶部２０２に記憶されてもよい。また、共通鍵Ｌ

は記憶部２０２に記憶される。

【０１４７】

Ｓｔｅｐ４－３）鍵生成装置１０の鍵生成処理部１０２は、公開鍵ｐｋとマスター秘密鍵ｍｓｋと属性ｙとを入力として、本実施形態に係る暗号文ポリシー属性ベースＫＥＭの鍵生成アルゴリズムＫｅｙＧｅｎを実行する。これにより、属性付き秘密鍵sk_yが生成される。属性付き秘密鍵sk_yは、例えば、通信ネットワークＮを介して復号装置３０に送信される。

【０１４８】

Ｓｔｅｐ４－４）復号装置３０の復号処理部３０１は、公開鍵ｐｋとポリシー付き暗号文ct_xと属性付き秘密鍵sk_yとを入力として、本実施形態に係る暗号文ポリシー属性ベースＫＥＭの復号アルゴリズムＤｅｃを実行する。これにより、復号失敗を示す⊥又は共通鍵Ｌ´のいずれかが出力される。この出力結果は、例えば、記憶部３０２に記憶される。

【０１４９】

＜鍵生成装置１０、暗号化装置２０及び復号装置３０のハードウェア構成＞

次に、本実施形態に係る暗号システム１に含まれる鍵生成装置１０、暗号化装置２０及び復号装置３０のハードウェア構成について、図２を参照しながら説明する。図２は、本実施形態に係る鍵生成装置１０、暗号化装置２０及び復号装置３０のハードウェア構成の一例を示す図である。なお、本実施形態に係る鍵生成装置１０、暗号化装置２０及び復号装置３０は同様のハードウェア構成で実現可能であるため、以降では、主に、鍵生成装置１０のハードウェア構成について説明する。

【０１５０】

図２に示すように、本実施形態に係る鍵生成装置１０は、入力装置５０１と、表示装置５０２と、ＲＡＭ（Random Access Memory）５０３と、ＲＯＭ（Read Only Memory）５０４と、プロセッサ５０５と、外部Ｉ／Ｆ５０６と、通信Ｉ／Ｆ５０７と、補助記憶装置５０８とを有する。これら各ハードウェアは、それぞれがバス５０９を介して通信可能に接続されている。

【０１５１】

入力装置５０１は、例えばキーボードやマウス、タッチパネル等である。表示装置５０２は、例えばディスプレイ等である。なお、鍵生成装置１０、暗号化装置２０及び復号装置３０は、入力装置５０１及び表示装置５０２のうちの少なくとも一方を有していなくてもよい。

【０１５２】

ＲＡＭ５０３は、プログラムやデータを一時保持する揮発性の半導体メモリである。ＲＯＭ５０４は、電源を切ってもプログラムやデータを保持することができる不揮発性の半導体メモリである。プロセッサ５０５は、例えばＣＰＵ（Central Processing Unit）等であり、ＲＯＭ５０４や補助記憶装置５０８等からプログラムやデータをＲＡＭ５０３上に読み出して処理を実行する演算装置である。

【０１５３】

外部Ｉ／Ｆ５０６は、外部装置とのインタフェースである。外部装置には、例えば、ＣＤ（Compact Disc）やＤＶＤ（Digital Versatile Disk）、ＳＤメモリカード（Secure Digital memory card）、ＵＳＢ（Universal Serial Bus）メモリカード等の記録媒体５０６ａ等がある。

【０１５４】

通信Ｉ／Ｆ５０７は、通信ネットワークに接続して他の装置と通信を行うためのインタフェースである。補助記憶装置５０８は、例えばＨＤＤ（Hard Disk Drive）やＳＳＤ（Solid State Drive）等の不揮発性の記憶装置である。

【０１５５】

本実施形態に係る鍵生成装置１０、暗号化装置２０及び復号装置３０は、図２に示すハードウェア構成を有することにより、上述した各アルゴリズムを実行して各種処理を実現

することができる。なお、図２では、本実施形態に係る鍵生成装置１０、暗号化装置２０及び復号装置３０が１台の装置（コンピュータ）で実現されている場合を示したが、これに限られない。本実施形態に係る鍵生成装置１０、暗号化装置２０及び復号装置３０は、複数台の装置（コンピュータ）で実現されていてもよい。また、１台の装置（コンピュータ）には、複数のプロセッサ５０５や複数のメモリ（ＲＡＭ５０３やＲＯＭ５０４、補助記憶装置５０８等）が含まれていてもよい。

【０１５６】

＜まとめ＞

以上のように、本実施形態に係る暗号システム１では、「本実施形態に係る鍵ポリシー属性ベース暗号」、「本実施形態に係る暗号文ポリシー属性ベース暗号」、「本実施形態に係る鍵ポリシー属性ベースＫＥＭ」及び「本実施形態に係る暗号文ポリシー属性ベースＫＥＭ」を実現することができる。これらの暗号方式及びＫＥＭ方式は、効率的である一方で表現力はＯＴ方式に比べると低いＦＡＭＥと呼ばれる方式の構成技術をベースにしている。なお、ＦＡＭＥの詳細については、例えば、文献「S. Agrawal and M. Chase. FAME: Fast attribute-based message encryption. In ACM CCS, 2017.」を参照されたい。

【０１５７】

ＦＡＭＥは効率的な構成である一方でポリシーを表現する条件式の中で否定を使うことができなかった。これに対して、本実施形態に係る暗号方式（及びこの暗号方式を応用したＫＥＭ方式）では、ＦＡＭＥの構造を参考に効率的に動作する性質を保ちながら、条件式の否定と属性ラベルの複数回出現とを可能にするように設計している。これにより、本実施形態に係る暗号システム１は、暗号文や秘密鍵のサイズを増大させずに任意の条件式をポリシーとして利用可能で、かつ、効率的な属性ベース暗号（及びこの属性ベース暗号を応用したＫＥＭ）を実現することができる。

【０１５８】

より具体的には、本実施形態に係る暗号システム１が実現する属性ベース暗号（及びこの属性ベース暗号を応用したＫＥＭ）では、第一に、ＯＴ方式と比較して暗号文と秘密鍵の群要素の数が減っているため、暗号化及び鍵生成時の比較的重い計算であるべき乗計算の回数を大きく減らすことができる。したがって、暗号化及び鍵生成の計算時間を削減することができる。

【０１５９】

また、第二に、復号時に必要な重い計算であるペアリング演算の回数も大きく減るため、復号もＯＴ方式に比べて高速である。特に、ペアリング演算の回数は利用されるポリシーにもよるが、高速なケースではそのポリシーの変数の数倍以上の速さの復号が可能である。例えば、２０個の変数からなるポリシーを持つ暗号文又は秘密鍵を用いて復号処理を行う場合、２０倍以上の高速化が可能である。

【０１６０】

更に、本実施形態に係る暗号システム１が実現する属性ベース暗号（及びこの属性ベース暗号を応用したＫＥＭ）では、暗号文や鍵のサイズを増大させることなく、任意の条件式をポリシーとして利用可能である。すなわち、条件式の中に属性ラベルが任意の回数出てきてもよい。

【０１６１】

本発明は、具体的に開示された上記の実施形態に限定されるものではなく、請求の範囲の記載から逸脱することなく、種々の変形や変更等が可能である。

【符号の説明】

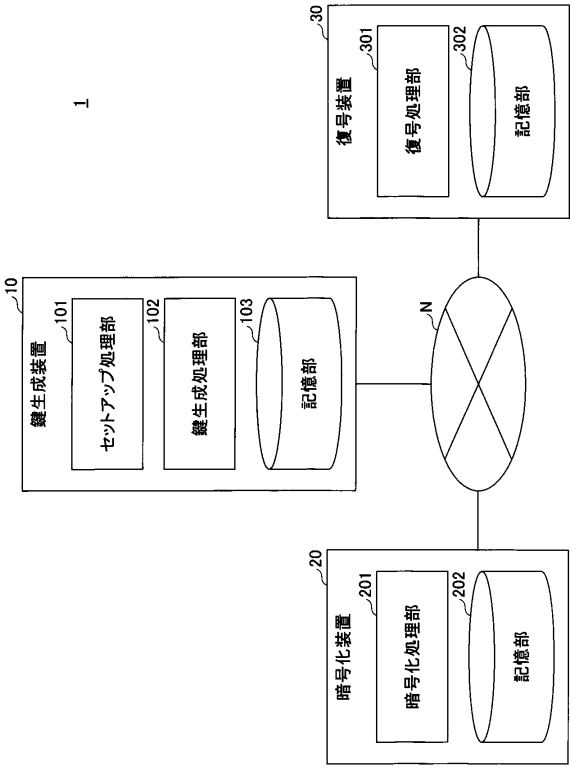
【０１６２】

１　暗号システム
１０　鍵生成装置
２０　暗号化装置
３０　復号装置

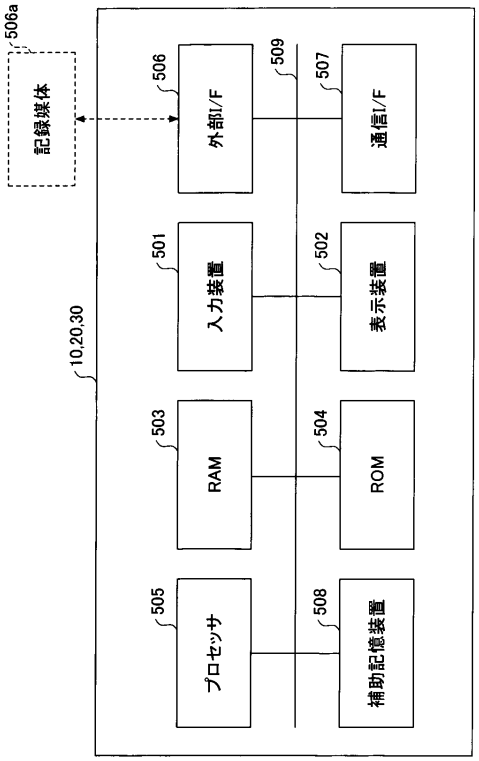
１０１　セットアップ処理部
１０２　鍵生成処理部
１０３　記憶部
２０１　暗号化処理部
２０２　記憶部
３０１　復号処理部
３０２　記憶部

【図面】

【図１】



【図２】



フロントページの続き

(56)参考文献 米国特許出願公開第２０１６／００１４０９５（ＵＳ，Ａ１）
国際公開第２０１５／１２５２９３（WO，Ａ１）
特開２０１６－１５５７１（ＪＰ，Ａ）
市川 幸宏 ほか，関数型暗号アプリケーションにおける適切な述語付与方式の検討，情報処理学会研究報告 ２０１２（平成２４）年度▲６▼［ＤＶＤ－ＲＯＭ］，日本，一般社団法人情報処理学会，2013年04月15日，Vol.2013-DPS-15 No.5，p. 1-6
石橋 拓哉 ほか，属性ベース暗号を用いたファイル共有サービスの複数組織対応に関する考察，電子情報通信学会技術研究報告，日本，一般社団法人電子情報通信学会，2018年02月26日，Vol.117 No.471，p.79-84

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０９Ｃ １／００
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ
ＴＨＥ ＡＣＭ ＤＩＧＩＴＡＬ ＬＩＢＲＡＲＹ