(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
2017年11月30日(30.11.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/203743 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *G09C 1/00* (2006.01)

(21) 国際出願番号： PCT/JP2017/001558

(22) 国際出願日： 2017年1月18日(18.01.2017)

(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 2016-106653 2016年5月27日(27.05.2016) JP

(71) 出願人:三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

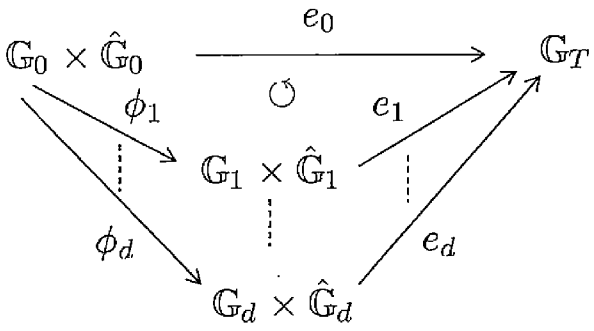
(72) 発明者: 高島 克幸 (**TAKASHIMA, Katsuyuki**); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 小柴 健史 (**KOSHIBA, Takeshi**); 〒3388570 埼玉県さいたま市桜区下大久保２５５ 国立大学法人埼玉大学内 Saitama (JP).

(74) 代理人: 溝井国際特許業務法人(**MIZOI INTERNATIONAL PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号３階 Kanagawa (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) **Title:** CIPHER APPARATUS, DECODING APPARATUS, AND CIPHER SYSTEM

(54) 発明の名称： 暗号化装置、復号装置及び暗号システム



(57) **Abstract:** The purpose of this invention is to make it possible to configure cipher such as attribute-based cipher that is effective even in the case where a quantum computer is made. A cipher system (1) uses a plurality of groups that are associated by an isogeny φ_t regarding an integer t of $t \in [d]$ and a pairing computation e_t regarding an integer t of $t \in [0, d]$. The cipher system (1) is provided with: a cipher apparatus (20) that generates ciphertext including a cipher element of a certain group among the plurality of groups; and a decoding apparatus (30) that decodes the ciphertext generated by the cipher apparatus (20) using a decoding key including a key element of a group different from the certain group among the plurality of groups.

(57) 要約：この発明は、量子計算機ができた場合にも有効な属性ベース暗号といった暗号を構成可能とすることを目的とする。暗号システム（１）は、ｔ∈［ｄ］の整数ｔについての同種写像φ_tと、ｔ∈［０，ｄ］の整数ｔについてのペアリング演算e_tとによって対応付けられた複数の群を用いる。暗号システム（１）は、複数の群のうちのある群の暗号要素を含む暗号文を生成する暗号化装置（２０）と、複数の群のうちの前記ある群とは異なる群の鍵要素を含む復号鍵を用いて、暗号化装置（２０）によって生成された暗号文を復号する復号装置（３０）とを備える。

WO 2017/203743 A1

［続葉有］

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

添付公開書類:

一 国際調査報告(条約第21条(3))

明　細　書

発明の名称 ： 暗号化装置、復号装置及び暗号システム

技術分野

[0001] この発明は、耐量子暗号方式に関する。

背景技術

[0002] 量子計算機の開発が世界的に進められている。量子計算機に対しても安全性を維持できる、すなわち耐量子性を有する、格子暗号をはじめとした暗号方式の研究も進められている。しかし、格子暗号には、的確なデータサイズ設定が未だ困難であるという指摘があり、他の数学原理に基づいた構成法が望まれていた。

[0003] 楕円曲線におけるペアリング演算を用いた属性ベース暗号（以下、ＡＢＥ）が数多く提案されている。非特許文献１には、楕円曲線におけるペアリング演算を用いた属性ベース暗号の１つの方式が記載されている。

[0004] また、非特許文献２には、同種写像を用いた、耐量子性を有する公開鍵暗号方式が記載されている。

先行技術文献

非特許文献

[0005] 非特許文献1：Ｖ．Ｇｏｙａｌ，　Ｏ．Ｐａｎｄｅｙ，　Ａ．Ｓａｈａｉ，　Ｂ．Ｗａｔｅｒｓ，　Ａｔｔｒｉｂｕｔｅ－ｂａｓｅｄ　ｅｎｃｒｙｐｔｉｏｎ　ｆｏｒ　ｃｉｒｃｕｉｔｓ

非特許文献2：Ｌ．Ｄｅ　Ｆｅｏ，　Ｄ．Ｊａｏ，　Ｊ．Ｐｌｕｔ，　Ｔｏｗａｒｄｓ　ｑｕａｎｔｕｍ－ｒｅｓｉｓｔａｎｔ　ｃｒｙｐｔｏｓｙｓｔｅｍｓ　ｆｒｏｍ　ｓｕｐｅｒｓｉｎｇｕｌａｒ　ｅｌｌｉｐｔｉｃ　ｃｕｒｖｅ　ｉｓｏｇｅｎｉｅｓ

非特許文献3：Ｄｅ　Ｆｅｏ，　Ｌ．，　Ｊａｏ，　Ｄ．，　Ｐｌｕｔ，　Ｊ．：　Ｔｏｗａｒｄｓ　ｑｕａｎｔｕｍ－ｒｅｓｉｓｔａｎｔ　ｃｒｙｐｔｏｓｙｓｔｅｍｓ　ｆｒｏｍ　ｓｕｐｅｒｓｉｎｇｕｌａｒ　ｅｌｌｉｐｔ

ic curve isogenies. J. Math. Crypt. 8(3), 209−247 (2014), preliminary version: IACR Cryptology eprint Archiv, 2011:506, 2011

非特許文献4：Charles, D., Lauter, K., Goren, E.: Cryptographic hash functions from expander graphs. J. Crypt. 22(1), 93−113 (2009), preliminary version: IACR Cryptology eprint Archiv, 2006:021, 2006

非特許文献5：Yoshida, R., Takashima, K.: Computing a sequence of 2−isogenies on supersingular elliptic curves. IEICE Trans. Fundamentals 96−A(1), 158−165 (2013), preliminary version is available in ICISC 2008, LNCS, vol. 5461, pp. 52−65 (2008)

発明の概要

発明が解決しようとする課題

[0006] しかし、楕円曲線ペアリングを用いた属性ベース暗号は全て、量子計算機によりマスター秘密鍵が暴かれ壊滅的な被害を受けることがわかっている。また、耐量子性を有する属性ベース暗号はなかった。

この発明は、量子計算機ができた場合にも有効な属性ベース暗号といった暗号方式を構成可能とすることを目的とする。

課題を解決するための手段

[0007] この発明に係る暗号化装置は、

同種写像とペアリング演算とによって対応付けられた複数の群を用いた暗号システムにおける暗号化装置であり、

前記複数の群のうちのある群の暗号要素を含む暗号文を生成する暗号文生成部を備える。

発明の効果

[0008] この発明では、同種写像とペアリング演算とによって対応付けられた複数の群を用いることにより、量子計算機ができた場合にも有効な属性ベース暗号といった暗号を構成可能となる。

図面の簡単な説明

[0009] [図1]実施の形態１に係るＩＢＥ方式で用いられる同種ペアリンググループの説明図。

[図2]実施の形態１に係る暗号システム１の構成図。

[図3]実施の形態１に係る鍵生成装置１０の構成図。

[図4]実施の形態１に係る暗号化装置２０の構成図。

[図5]実施の形態１に係る復号装置３０の構成図。

[図6]実施の形態１に係るＳｅｔｕｐアルゴリズムのフローチャート。

[図7]実施の形態１に係る同種ペアリンググループの説明図。

[図8]実施の形態１に係るＫｅｙＧｅｎアルゴリズムのフローチャート。

[図9]実施の形態１に係るＥｎｃアルゴリズムのフローチャート。

[図10]実施の形態１に係るＤｅｃアルゴリズムのフローチャート。

[図11]実施の形態１に係るＩＢＥ方式に対する攻撃法の説明図。

[図12]変形例１に係る鍵生成装置１０の構成図。

[図13]変形例１に係る暗号化装置２０の構成図。

[図14]変形例１に係る復号装置３０の構成図。

[図15]実施の形態２に係る暗号システム１の構成図。

[図16]実施の形態２に係る鍵生成装置１０の構成図。

[図17]実施の形態２に係る暗号化装置２０の構成図。

[図18]実施の形態２に係る復号装置３０の構成図。

[図19]実施の形態５に係るＩＰＧ生成アルゴリズムのフローチャート。

[図20]実施の形態５に係るアルゴリズム$\mathrm{Isog}_{L\sim,\kappa}(E_0)$の説明図。

[図21]実施の形態５に係るアルゴリズムＩｓｏｇ$_{L\sim,\kappa}$（Ｅ$_0$）の説明図。

発明を実施するための形態

[0010] 実施の形態１.

実施の形態１では、耐量子性を有するＩＤベース暗号（以下、ＩＢＥ）方式について説明する。

[0011] ＊＊＊記法の説明＊＊＊

実施の形態１で用いられる記法について説明する。

[0012] Ａがランダムな値または分布であるとき、数１０１は、Ａの分布に従いＡからｙをランダムに選択することを表す。つまり、数１０１において、ｙは乱数である。

[数101]

$$y \xleftarrow{R} A$$

[0013] Ａが集合であるとき、数１０２は、Ａからｙを一様に選択することを表す。つまり、数１０２において、ｙは一様乱数である。

[数102]

$$y \xleftarrow{U} A$$

[0014] 数１０３は、位数ｑの体を表す。

[数103]

$$\mathbb{F}_q$$

また、位数ｑの体を文中では単にＦ$_q$と記載する。

[0015] ［ｎ］：＝｛１，．．．，ｎ｝とし、［０，ｎ］：＝｛０｝∪［ｎ］：＝｛０，．．．，ｎ｝とする。ｎは、０以上の整数である。

[0016] 数１０４に示す２つのベクトルｙ→及びｖ→について、ｙ→・ｖ→は、数１０５に示す内積を示す。

[数104]

$$\vec{y} = (y_i)_{i \in [r]},\ \vec{v} = (v_i)_{i \in [r]}$$

[数105]

$$\sum_{i=1}^{r} y_i v_i$$

[0017] ＊＊＊概念の説明＊＊＊

図１を参照して、実施の形態１に係るＩＢＥ方式で用いられる同種ペアリンググループ（以下、ＩＰＧ）について説明する。

[0018] ＩＰＧは、同種写像とペアリング演算とによって対応付けられた複数の群を有する。

具体的には、ＩＰＧは、群G_0と、群G_0と同種写像ϕ_tによって対応付けられたｔ＝１，．．．，ｄの各群G_tと、ｔ＝０，．．．，ｄの各群G_t及び群$\hat{G}_t$とペアリング演算e_tによって対応付られた群G_Tとを有する。そして、ＩＰＧでは、群G_0×群$\hat{G}_0$からペアリング演算e_0で変換された場合と、ｔ＝１，．．．，ｄのいずれの整数ｔについての同種写像ϕ_tによって群G_0×群$\hat{G}_0$から群G_t×群$\hat{G}_t$に変換された上で、ペアリング演算e_tによって変換された場合とで、結果は等しくなる。

[0019] より正確には、ＩＰＧは以下のように定義される。

ＩＰＧ生成アルゴリズム$Gen^{IPG}(1^{\lambda}, d)$では、数１０６に示す公開パラメータ$pk^{IPG}$とマスター秘密鍵$sk^{IPG}$とのマスター鍵ペアがランダムに生成される。

[数106]

$$\begin{aligned} &Gen^{IPG}(1^{\lambda}, d) \\ &\xrightarrow{R} (pk^{IPG} := ((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t\in[0,d]}, \mathbb{G}_T)), \\ &\qquad sk^{IPG} := (\phi_t)_{t\in[d]}) \end{aligned}$$

ここで、（G_t，$\hat{G}_t$，e_t，G_T）は、ペアリング演算$e_t : G_t \times \hat{G}_t \to G_T$を有する素数位数ｑの非対称ペアリング群である。$\hat{g}_t \in \hat{G}_t$である。同種写像$\phi_t : G_0 \to G_t$であり、異なる楕円曲線間の同種によって与えられる。$g_t = \phi_t(g_0) \in G_t$である。

ＩＰＧは、数１０７に示す両立性を有する。

[数107]

$$e_0(g_0,\hat{g}_0)=e_t(g_t,\hat{g}_t)=e_t(\phi_t(g_0),\hat{g}_t) \quad \text{for any } t\in[d]$$

ここで、$g_T=e_0(g_0, \hat{g}_0)\neq 1$である。また、$G_t\neq\hat{G}_t$である。

[0020] ＊＊＊構成の説明＊＊＊

実施の形態１に係るＩＢＥ方式の構成を説明する。

ＩＢＥ方式は、Ｓｅｔｕｐアルゴリズムと、ＫｅｙＧｅｎアルゴリズムと、Ｅｎｃアルゴリズムと、Ｄｅｃアルゴリズムとを備える。

Ｓｅｔｕｐアルゴリズムは、セキュリティパラメータ1^{λ}を入力として、公開パラメータｐｋと、マスター秘密鍵ｓｋとを出力する。

ＫｅｙＧｅｎアルゴリズムは、公開パラメータｐｋと、マスター秘密鍵ｓｋと、識別子ＩＤとを入力として、識別子ＩＤに対応した復号鍵sk_{ID}を出力する。

Ｅｎｃアルゴリズムは、公開パラメータｐｋと、メッセージ空間ｍｓｇにおけるメッセージｍと、識別子ＩＤ’とを入力として、暗号文$ct_{ID'}$を出力する。

Ｄｅｃアルゴリズムは、公開パラメータｐｋと、識別子ＩＤに対応した復号鍵sk_{ID}と、識別子ＩＤ’の下で暗号化された暗号文$ct_{ID'}$とを入力として、メッセージｍ’∈ｍｓｇ、又は、復号に失敗したことを示す識別情報⊥を出力する。

[0021] 図２を参照して、実施の形態１に係る暗号システム１の構成を説明する。

暗号システム１は、鍵生成装置１０と、暗号化装置２０と、復号装置３０とを備える。

鍵生成装置１０と暗号化装置２０と復号装置３０とは、コンピュータである。鍵生成装置１０と暗号化装置２０と復号装置３０とは、ネットワークを介して接続されている。

[0022] 鍵生成装置１０は、セキュリティパラメータ1^{λ}を入力として、Ｓｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋと、マスター秘密鍵ｓｋとを

生成する。また、鍵生成装置１０は、公開パラメータｐｋと、マスター秘密鍵ｓｋと、識別子ＩＤとを入力として、ＫｅｙＧｅｎアルゴリズムを実行して、復号鍵sk_{ID}を生成する。

鍵生成装置１０は、公開パラメータｐｋを公開し、復号鍵sk_{ID}を識別子ＩＤに対応する復号装置３０に出力する。鍵生成装置１０は、マスター秘密鍵ｓｋを保管する。

[0023] 暗号化装置２０は、公開パラメータｐｋと、メッセージｍと、識別子ＩＤ’とを入力として、Ｅｎｃアルゴリズムを実行して、暗号文$ct_{ID'}$を生成する。暗号化装置２０は、暗号文$ct_{ID'}$を復号装置３０に出力する。

[0024] 復号装置３０は、公開パラメータｐｋと、復号鍵sk_{ID}と、暗号文$ct_{ID'}$とを入力として、Ｄｅｃアルゴリズムを実行して、メッセージｍ’、又は、復号に失敗したこと

を示す識別情報⊥を生成する。

[0025] 図３を参照して、実施の形態１に係る鍵生成装置１０の構成を説明する。

鍵生成装置１０は、プロセッサ１１と、記憶装置１２と、入出力インタフェース１３とのハードウェアを備える。プロセッサ１１は、信号線を介して他のハードウェアと接続され、これら他のハードウェアを制御する。

[0026] 鍵生成装置１０は、機能構成要素として、マスター鍵生成部１４と、復号鍵生成部１５と、鍵出力部１６とを備える。マスター鍵生成部１４と、復号鍵生成部１５と、鍵出力部１６との各部の機能はソフトウェアにより実現される。

記憶装置１２には、鍵生成装置１０の各部の機能を実現するプログラムが記憶されている。このプログラムは、プロセッサ１１により読み込まれ、プロセッサ１１によって実行される。これにより、鍵生成装置１０の各部の機能が実現される。

[0027] 図４を参照して、実施の形態１に係る暗号化装置２０の構成を説明する。

暗号化装置２０は、プロセッサ２１と、記憶装置２２と、入出力インタフェース２３とのハードウェアを備える。プロセッサ２１は、信号線を介して

他のハードウェアと接続され、これら他のハードウェアを制御する。

[0028] 暗号化装置２０は、機能構成要素として、入力受付部２４と、暗号文生成部２５と、暗号文出力部２６とを備える。入力受付部２４と、暗号文生成部２５と、暗号文出力部２６との各部の機能はソフトウェアにより実現される。

記憶装置２２には、暗号化装置２０の各部の機能を実現するプログラムが記憶されている。このプログラムは、プロセッサ２１により読み込まれ、プロセッサ２１によって実行される。これにより、暗号化装置２０の各部の機能が実現される。

[0029] 図５を参照して、実施の形態１に係る復号装置３０の構成を説明する。

復号装置３０は、プロセッサ３１と、記憶装置３２と、入出力インタフェース３３とのハードウェアを備える。プロセッサ３１は、信号線を介して他のハードウェアと接続され、これら他のハードウェアを制御する。

[0030] 復号装置３０は、機能構成要素として、入力受付部３４と、復号部３５と、メッセージ出力部３６とを備える。入力受付部３４と、復号部３５と、メッセージ出力部３６との各部の機能はソフトウェアにより実現される。

記憶装置３２には、復号装置３０の各部の機能を実現するプログラムが記憶されている。このプログラムは、プロセッサ３１により読み込まれ、プロセッサ３１によって実行される。これにより、復号装置３０の各部の機能が実現される。

[0031] プロセッサ１１，２１，３１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）である。プロセッサ１１，２１，３１は、具体例としては、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）、ＧＰＵ（Ｇｒａｐｈｉｃｓ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。

[0032] 記憶装置１２，２２，３２は、具体例としては、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ

Ｍｅｍｏｒｙ）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）である。ま

た、記憶装置１２，２２，３２は、ＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）メモリカード、ＣＦ（ＣｏｍｐａｃｔＦｌａｓｈ）、ＮＡＮＤフラッシュ、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、ＤＶＤといった可搬記憶媒体であってもよい。

[0033] 入出力インタフェース１３，２３，３３は、外部からデータの入力を受け付け、外部へデータを出力するためのインタフェースである。入出力インタフェース１３，２３，３３は、具体例としては、キーボードといった入力装置と、ディスプレイといった出力装置とを接続するＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）、ＰＳ／２、ＨＤＭＩ（登録商標、Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ　Ｍｕｌｔｉｍｅｄｉａ　Ｉｎｔｅｒｆａｃｅ）といったコネクタである。また、入出力インタフェース１３，２３，３３は、具体例としては、外部からネットワークを介してデータを送受信するＮＩＣ（Ｎｅｔｗｏｒｋ

Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）であってもよい。

[0034] プロセッサ１１によって実現される各部の機能の処理の結果を示す情報とデータと信号値と変数値は、記憶装置１２、又は、プロセッサ１１内のレジスタ又はキャッシュメモリに記憶される。同様に、プロセッサ２１によって実現される各部の機能の処理の結果を示す情報とデータと信号値と変数値は、記憶装置２２、又は、プロセッサ２１内のレジスタ又はキャッシュメモリに記憶される。同様に、プロセッサ３１によって実現される各部の機能の処理の結果を示す情報とデータと信号値と変数値は、記憶装置３２、又は、プロセッサ３１内のレジスタ又はキャッシュメモリに記憶される。

[0035] プロセッサ１１によって実現される各機能を実現するプログラムは、記憶装置１２に記憶されているとした。同様に、プロセッサ２１によって実現される各機能を実現するプログラムは、記憶装置２２に記憶されているとした。同様に、プロセッサ３１によって実現される各機能を実現するプログラムは、記憶装置３２に記憶されているとした。しかし、このプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブ

ルーレイ（登録商標）ディスク、ＤＶＤといった可搬記憶媒体に記憶されてもよい。

[0036] 図３では、プロセッサ１１は、１つだけ示されていた。しかし、鍵生成装置１０は、プロセッサ１１を代替する複数のプロセッサを備えていてもよい。これら複数のプロセッサは、鍵生成装置１０の各部の機能を実現するプログラムの実行を分担する。それぞれのプロセッサは、プロセッサ１１と同じように、プロセッシングを行うＩＣである。同様に、暗号化装置２０は、プロセッサ２１を代替する複数のプロセッサを備えていてもよい。また、復号装置３０は、プロセッサ３１を代替する複数のプロセッサを備えていてもよい。

[0037] ＊＊＊動作の説明＊＊＊

図３から図９を参照して、実施の形態１に係る暗号システム１の動作を説明する。

実施の形態１に係る暗号システム１の動作は、実施の形態１に係る暗号方法に相当する。また、実施の形態１に係る暗号システム１の動作は、実施の形態１に係る暗号プログラムの処理に相当する。

[0038] 図３及び図６を参照して、実施の形態１に係るＳｅｔｕｐアルゴリズムを説明する。

Ｓｅｔｕｐアルゴリズムは、鍵生成装置１０によって実行される。

[0039] （ステップＳ１１：ＩＰＧ生成処理）

マスター鍵生成部１４は、入出力インタフェース１３を介してセキュリティパラメータ1^{λ}の入力を受け付ける。マスター鍵生成部１４は、受け付けられたセキュリティパラメータ1^{λ}と、ｄ＝１とを入力として、ＩＰＧ生成アルゴリズム$\mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda}, d)$を実行して、数１０８に示す公開パラメータ$\mathrm{pk}^{\mathrm{IPG}}$とマスター秘密鍵$\mathrm{sk}^{\mathrm{IPG}}$とのマスター鍵ペアを生成する。

[数108]

$$(\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T)),\ \mathrm{sk}^{\mathrm{IPG}} := \phi_1) \xleftarrow{R} \mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda}, 1)$$

[0040] つまり、図７に示すように、実施の形態１では、ｔ＝０，１についての群G_t及び群$\hat{G}_t$とペアリング演算e_tと、群G_Tと、同種写像ϕ_1とが生成される。

なお、図７に示されるように、G_0からG_1への変換が“復号鍵生成（ＫｅｙＧｅｎ）”に、$G_0 \times \hat{G}_0$からG_Tへの変換が“暗号化（Ｅｎｃ）”に、$G_1 \times \hat{G}_1$からG_Tへの変換が“復号（Ｄｅｃ）”に大まかに対応している。

[0041] （ステップＳ１２：ハッシュ関数生成処理）

マスター鍵生成部１４は、識別子の空間である体F_qの要素を、群G_0の要素に変換するランダムなハッシュ関数Ｈを生成する。

[0042] （ステップＳ１３：マスター鍵生成処理）

マスター鍵生成部１４は、ステップＳ１１で生成された公開パラメータpk^{IPG}と、ステップＳ１２で生成されたハッシュ関数Ｈとを用いて、公開パラメータ$pk := ((G_t, \hat{G}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, G_T, H)$を生成する。鍵出力部１６は、公開パラメータｐｋを入出力インタフェース１３を介して外部の公開用サーバ等へ出力することにより、公開パラメータｐｋを暗号化装置２０及び復号装置３０に出力する。

また、マスター鍵生成部１４は、ステップＳ１１で生成されたマスター秘密鍵sk^{IPG}を用いて、マスター秘密鍵$sk := \phi_1$を生成する。マスター鍵生成部１４は、生成されたマスター秘密鍵ｓｋを記憶装置１２に書き込む。

[0043] つまり、マスター鍵生成部１４は、数１０９に示すＳｅｔｕｐアルゴリズムを実行して、マスター鍵ペアを生成する。

[数109]

$$\begin{aligned}
&\mathrm{Setup}(1^\lambda):\\
&(\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T)),\ \mathrm{sk}^{\mathrm{IPG}} := \phi_1)\\
&\qquad\qquad \xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}(1^\lambda, 1),\\
&\text{generate a random hash } H : \mathbb{F}_q \to \mathbb{G}_0 \text{ with the identity space } \mathbb{F}_q,\\
&\text{return pk} := ((\mathbb{G}_t, \hat{\mathbb{G}}_t, \hat{g}_t, e_t)_{t=0,1}, \mathbb{G}_T, H),\ \mathrm{sk} := \phi_1.
\end{aligned}$$

[0044] 図３及び図８を参照して、実施の形態１に係るＫｅｙＧｅｎアルゴリズムを説明する。

ＫｅｙＧｅｎアルゴリズムは、鍵生成装置１０によって実行される。

[0045] （ステップＳ２１：ＩＤ受付処理）

復号鍵生成部１５は、入出力インタフェース１３を介して、復号鍵sk_{ID}を使用するユーザの識別子ＩＤの入力を受け付ける。

[0046] （ステップＳ２２：鍵要素生成処理）

復号鍵生成部１５は、ステップＳ２１で受け付けられた識別子ＩＤを入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈを計算して、群G_0の要素である要素h_0を生成する。復号鍵生成部１５は、マスター秘密鍵ｓｋに含まれる同種写像ϕ_1で要素h_0を変換して、要素h_1を生成する。

[0047] （ステップＳ２３：鍵要素出力処理）

鍵出力部１６は、ステップＳ２１で受け付けられた識別子ＩＤと、ステップＳ２２で生成された要素h_1とを鍵要素とする復号鍵sk_{ID}を、入出力インタフェース１３を介して復号装置３０に出力する。この際、鍵出力部１６は、何らかの暗号方式で暗号化するといった方法により、復号鍵sk_{ID}が第三者に漏えいしないようにする。

[0048] つまり、復号鍵生成部１５は、数１１０に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵sk_{ID}を生成する。

[数110]

$$\begin{aligned}&\mathrm{KeyGen}(\mathrm{pk}, \mathrm{sk}, \mathrm{ID}):\\&h_0 := H(\mathrm{ID}) \in \mathbb{G}_0,\ h_1 := \phi_1(h_0),\\&\mathrm{return}\ \mathrm{sk}_{\mathrm{ID}} := (\mathrm{ID}, h_1).\end{aligned}$$

[0049] 図４及び図９を参照して、実施の形態１に係るＥｎｃアルゴリズムを説明する。

Ｅｎｃアルゴリズムは、暗号化装置２０によって実行される。

[0050] （ステップＳ３１：入力受付処理）

入力受付部２４は、入出力インタフェース２３を介して、鍵生成装置１０

によって生成された公開パラメータｐｋと、暗号化対象のメッセージｍと、復号条件となる識別子ＩＤ’との入力を受け付ける。

[0051] （ステップＳ３２：暗号文生成処理）

暗号文生成部２５は、ステップＳ３１で受け付けられた識別子ＩＤ’を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈを計算して、群G_0の要素である要素h_0を生成する。また、暗号文生成部２５は、一様乱数ζを生成する。

暗号文生成部２５は、一様乱数ζを用いて、数１１１に示す要素ｃを生成する。

[数111]

$$c := \hat{g}_1^{\zeta}$$

また、暗号文生成部２５は、要素h_0及び一様乱数ζを用いて、数１１２に示す要素ｚを生成する。そして、暗号文生成部２５は、ステップＳ３１で受け付けられたメッセージｍと、要素ｚを用いて要素c_T：＝ｚ・ｍを生成する。

[数112]

$$z := e_0(h_0, \hat{g}_0)^{\zeta}$$

[0052] （ステップＳ３３：暗号文出力処理）

暗号文出力部２６は、ステップＳ３１で受け付けられた識別子ＩＤ’と、ステップＳ３２で生成された要素ｃ，c_Tとを暗号要素とする暗号文$ct_{ID'}$を、入出力インタフェース２３を介して復号装置３０に出力する。

[0053] つまり、暗号化装置２０は、数１１３に示すＥｎｃアルゴリズムを実行して、暗号文$ct_{ID'}$を生成する。

[数113]

$$\begin{aligned}&\mathrm{Enc}(\mathrm{pk}, m, \mathrm{ID}'):\\&h_0 := H(\mathrm{ID}') \in \mathbb{G}_0,\ \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\mathrm{X}},\\&c := \hat{g}_1^{\zeta},\ z := e_0(h_0, \hat{g}_0)^{\zeta},\ c_T := z \cdot m,\\&\text{return } \mathrm{ct}_{\mathrm{ID}'} := (\mathrm{ID}',\ c,\ c_T).\end{aligned}$$

[0054] 図５及び図１０を参照して、実施の形態１に係るＤｅｃアルゴリズムを説明する。

Ｄｅｃアルゴリズムは、復号装置３０によって実行される。

[0055] （ステップＳ４１：入力受付処理）

入力受付部３４は、入出力インタフェース３３を介して、鍵生成装置１０によって生成された公開パラメータｐｋ及び復号鍵$\mathrm{sk}_{\mathrm{ID}}$と、暗号化装置２０によって生成された暗号文$\mathrm{ct}_{\mathrm{ID}'}$との入力を受け付ける。

[0056] （ステップＳ４２：復号判定処理）

復号部３５は、ステップＳ４１で受け付けられた復号鍵$\mathrm{sk}_{\mathrm{ID}}$に含まれる識別子ＩＤと、暗号文$\mathrm{ct}_{\mathrm{ID}'}$に含まれる識別子ＩＤ’とが等しいか否かを判定する。これにより、暗号文$\mathrm{ct}_{\mathrm{ID}'}$を復号鍵$\mathrm{sk}_{\mathrm{ID}}$で復号可能かが判定される。

復号部３５は、等しいと判定された場合、つまり復号可能と判定された場合、処理をステップＳ４３に進め、そうでない場合、処理をステップＳ４５に進める。

[0057] （ステップＳ４３：復号処理）

復号部３５は、ステップＳ４１で受け付けられた復号鍵$\mathrm{sk}_{\mathrm{ID}}$に含まれる要素$\mathrm{h}_1$と、暗号文$\mathrm{ct}_{\mathrm{ID}'}$に含まれる暗号要素ｃとについてペアリング演算$\mathrm{e}_1$を行い、要素ｚ’を計算する。復号部３５は、計算された要素ｚ’を用いて、メッセージｍ’：＝c_{T}・（ｚ’）$^{-1}$を計算する。

[0058] （ステップＳ４４：メッセージ出力処理）

メッセージ出力部３６は、ステップＳ４２で計算されたメッセージｍ’を

、入出力インタフェース３３を介して出力する。

[0059] （ステップＳ４５：識別情報出力処理）

メッセージ出力部３６は、識別情報⊥を、入出力インタフェース３３を介して出力する。

[0060] つまり、復号装置３０は、数１１４に示すＤｅｃアルゴリズムを実行して、暗号文$ct_{ID'}$を復号鍵sk_{ID}により復号する。

[数114]

$$\begin{aligned}&\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathrm{ID}}, \mathrm{ct}_{\mathrm{ID}'}):\\&\quad \text{if } (\mathrm{ID} = \mathrm{ID}'),\\&\quad\quad z' := e_1(h_1, c),\ m' := c_T \cdot (z')^{-1},\\&\quad\quad \text{return } m'.\\&\quad \text{otherwise, return } \perp.\end{aligned}$$

[0061] ＊＊＊実施の形態１の効果＊＊＊

以上のように、実施の形態１に係る暗号システム１は、ＩＰＧを用いてＩＢＥ方式を実現する。ここで、鍵生成装置１０によって生成されるマスター秘密鍵$sk := \phi_1$は、耐量子性を有している。そのため、量子計算機によってでも、マスター秘密鍵ｓｋが破られることがない。

[0062] 図１１を参照して、実施の形態１の効果を詳しく説明する。

実施の形態１に係るＩＢＥ方式は、秘密鍵が２階層の階層的な構造となっている。つまり、実施の形態１に係るＩＢＥ方式は、秘密鍵が、上位階層のマスター秘密鍵と、下位階層の復号鍵との２階層の構造となっている。

もし、マスター秘密鍵が明らかになると、どんな識別子ＩＤについての復号鍵も、従来の確率的多項式時間マシンを用いて生成可能になる。そのため、攻撃者は、効率的に攻撃するために、初めにマスター秘密鍵を明らかにしようとする。もしマスター秘密鍵が守られると、攻撃者は暗号文を１つ１つ破る必要がある。マスター秘密鍵を攻撃する方法を“マスター鍵レベルアタック”と呼び、暗号文を１つ１つ攻撃する方法を“ユーザレベルアタック”と呼ぶ。

量子計算機が開発された場合、実施の形態１に係る暗号システム１では、ユーザレベルアタックは可能になってしまうものの、マスター鍵レベルアタックは防ぐことができる。

仮に量子計算機が完成したとしても、初期の段階では、既存のコンピュータの場合と同様に、開発速度は比較的遅いものと考えられる。そして、少なくとも、初期の段階では、持ち運び可能なハンディタイプの量子計算機は広まらないし、そのような量子計算機は高額であると考えられる。そのため、ユーザレベルアタックは非常に非効率となると考えられる。実施の形態１に係る暗号システム１では、効率的なＩＢＥ方式を実現しつつ、マスター鍵レベルアタックは防ぐことができる。したがって、実施の形態１に係る暗号システム１で実現されるＩＢＥ方式は、仮に量子計算機が完成したとしても、しばらくの間は効率的かつ有用なものと考えられる。

[0063] ＊＊＊他の構成＊＊＊

＜変形例１＞

実施の形態１では、鍵生成装置１０、暗号化装置２０、復号装置３０の各部の機能がソフトウェアで実現された。変形例１として、鍵生成装置１０、暗号化装置２０、復号装置３０の各部の機能はハードウェアで実現されてもよい。この変形例１について、実施の形態１と異なる点を説明する。

[0064] 図１２から図１４を参照して、変形例１に係る鍵生成装置１０、暗号化装置２０、復号装置３０の構成を説明する。

各部の機能がハードウェアで実現される場合、鍵生成装置１０、暗号化装置２０、復号装置３０は、プロセッサ１１，２１，３１と記憶装置１２，２２，３２とに代えて、処理回路１７，２７，３７を備える。処理回路１７，２７，３７は、鍵生成装置１０、暗号化
装置２０、復号装置３０の各部の機能と、記憶装置１２，２２，３２の機能とを実現する専用の電子回路である。

[0065] 処理回路１７，２７，３７は、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ロジックＩＣ、ＧＡ（Ｇａｔ

ｅ　Ａｒｒａｙ）、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）が想定される。

鍵生成装置１０、暗号化装置２０、復号装置３０は、処理回路１７，２７，３７を代替する複数の処理回路を備えていてもよい。これら複数の処理回路により、全体として各部の機能が実現される。それぞれの処理回路は、処理回路１７，２７，３７と同じように、専用の電子回路である。

[0066] ＜変形例２＞

変形例２として、一部の機能がハードウェアで実現され、他の機能がソフトウェアで実現されてもよい。つまり、鍵生成装置１０、暗号化装置２０、復号装置３０の各部のうち、一部の機能がハードウェアで実現され、他の機能がソフトウェアで実現されてもよい。

[0067] プロセッサ１１，２１，３１と記憶装置１２，２２，３２と処理回路１７，２７，３７とを、総称して「プロセッシングサーキットリー」という。つまり、各部の機能は、プロセッシングサーキットリーにより実現される。

[0068] 実施の形態２．

実施の形態２では、耐量子性を有するＡＢＥ方式について説明する。実施の形態２では、実施の形態１と異なる点を説明する。

実施の形態２では、ｔ∈［ｄ］について（ｔ，１）∈［ｄ］×［１］＝［ｄ］×Ｕで特定される、多項式サイズのユニバース［ｄ］の要素として属性が与えられる場合を説明する。つまり、後述する属性集合Γ⊂［ｄ］の場合を説明する。

[0069] ＊＊＊概念の説明＊＊＊

実施の形態２に係るＡＢＥ方式で用いられる概念について説明する。

スパンプログラムについて説明する。スパンプログラムは既存の概念であるため、ここでは以下の説明で必要な範囲だけ簡単に説明する。

[0070] 体F_q上のスパンプログラムは、ラベル付けされた行列Ｓ：＝（Ｍ，ρ）である。ここで、行列Ｍは、体F_q上の（Ｌ行×ｒ列）の行列である。ラベルρ

は、｛（ｔ，ｖ），（ｔ’，ｖ’），．．．｝から属性に応じて行列Ｍの行に対して付されたラベルである。なお、全ての行が１つの属性にラベル付けされる。つまり、ρ：｛1，．．．，Ｌ｝→｛（ｔ，ｖ），（ｔ’，ｖ’），．．．｝である。

スパンプログラムは、以下の基準に従い、入力を受理又は拒絶する。Γを属性集合とする。つまり、$\Gamma := \{(t_j, x_j)\}_{1 \leq j \leq d'}$（$x_j \in U_{t_j}$）である。$1 \to \in span\langle (M_i)_{\rho(i) \in \Gamma} \rangle$の場合に限り、スパンプログラムＳは属性集合Γを受理する。スパンプログラムＳが属性集合Γを受理することを、Ｒ（Ｓ，Γ）＝１と表す。つまり、行列Ｍの行$(M_i)_{\rho(i) \in \Gamma}$の線形結合によって全ての要素が１のベクトルが得られる場合に限り、スパンプログラムＳは属性集合Γを受理する。行列Ｓをアクセスストラクチャと呼ぶ。

[0071] ＊＊＊構成の説明＊＊＊

実施の形態２では、復号鍵に復号条件であるポリシーが設定される鍵ポリシー型のＡＢＥ（以下、ＫＰ－ＡＢＥ）方式について説明する。なお、同様の考え方により、暗号文に
ポリシーが設定される暗号文ポリシー型のＡＢＥを実現することも可能である。

特に、実施の形態２では、タグ付されたＫＰ－ＡＢＥ方式について説明する。タグ付けされたＫＰ－ＡＢＥ方式では、復号鍵のパラメータ（ｔａｇ，Ｓ）と、暗号文のパラメータ（ｔａｇ’，Γ）とに対して、関係R^+（（ｔａｇ，Ｓ），（ｔａｇ’，Γ））：＝Ｅｑ（ｔａｇ，ｔａｇ’）∧Ｒ（Ｓ，Γ）と定義される。ここで、ｔａｇ＝ｔａｇ’の場合に限り、Ｅｑ（ｔａｇ，ｔａｇ’）＝１である。そして、Ｅｑ（ｔａｇ，ｔａｇ’）＝１∧Ｒ（Ｓ，Γ）＝１の場合に、暗号文を復号鍵で復号できる。

[0072] ＫＰ－ＡＢＥ方式は、Ｓｅｔｕｐアルゴリズムと、ＫｅｙＧｅｎアルゴリズムと、Ｅｎｃアルゴリズムと、Ｄｅｃアルゴリズムとを備える。

Ｓｅｔｕｐアルゴリズムは、セキュリティパラメータ1^λを入力として、公開パラメータｐｋと、マスター秘密鍵ｓｋとを出力する。

ＫｅｙＧｅｎアルゴリズムは、公開パラメータｐｋと、マスター秘密鍵ｓｋと、入力タグｔａｇと、アクセスストラクチャＳ：＝（Ｍ，ρ）とを入力として、入力タグｔａｇ及びアクセスストラクチャＳに対応した復号鍵$sk_{tag,S}$を出力する。

Ｅｎｃアルゴリズムは、公開パラメータｐｋと、メッセージ空間ｍｓｇにおけるメッセージｍと、入力タグｔａｇ’と、属性集合Γ：＝｛（t_j，x_j）｝$_{1\leqq j\leqq d'}$を入力として、暗号文$ct_{tag',\Gamma}$を出力する。

Ｄｅｃアルゴリズムは、公開パラメータｐｋと、入力タグｔａｇ及びアクセスストラクチャＳに対応した復号鍵$sk_{tag,S}$と、入力タグｔａｇ’及び属性集合Γの下で暗号化された暗号文$ct_{tag',\Gamma}$とを入力として、メッセージｍ’∈ｍｓｇ、又は、復号に失敗したことを示す識別情報⊥を出力する。

[0073] 図１５を参照して、実施の形態２に係る暗号システム１の構成を説明する。

暗号システム１は、鍵生成装置１０と、暗号化装置２０と、復号装置３０とを備える。

鍵生成装置１０と暗号化装置２０と復号装置３０とは、コンピュータである。鍵生成装置１０と暗号化装置２０と復号装置３０とは、ネットワークを介して接続されている。

[0074] 鍵生成装置１０は、セキュリティパラメータ1^{λ}を入力として、Ｓｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋと、マスター秘密鍵ｓｋとを生成する。また、鍵生成装置１０は、公開パラメータｐｋと、マスター秘密鍵ｓｋと、入力タグｔａｇと、アクセスストラクチャＳ：＝（Ｍ，ρ）とを入力として、ＫｅｙＧｅｎアルゴリズムを実行して、復号鍵$sk_{tag,S}$を生成する。

鍵生成装置１０は、公開パラメータｐｋを公開し、復号鍵$sk_{tag,S}$を入力タグｔａｇ及びアクセスストラクチャＳに対応する復号装置３０に出力する。鍵生成装置１０は、マスター秘密鍵ｓｋを保管する。

[0075] 暗号化装置２０は、公開パラメータｐｋと、メッセージｍと、入力タグｔ

ａｇ’と、属性集合Γとを入力として、Ｅｎｃアルゴリズムを実行して、暗号文$ｃｔ_{tag',Γ}$を生成する。暗号化装置２０は、暗号文$ｃｔ_{tag',Γ}$を復号装置３０に出力する。

[0076] 復号装置３０は、公開パラメータｐｋと、復号鍵$ｓｋ_{tag,S}$と、暗号文$ｃｔ_{tag',Γ}$とを入力として、Ｄｅｃアルゴリズムを実行して、メッセージm’、又は、復号に失敗したことを示す識別情報⊥を生成する。

[0077] 図１６に示す鍵生成装置１０と、図１７に示す暗号化装置２０と、図１８に示す復号装置３０との構成は、それぞれ図３に示す鍵生成装置１０と、図４に示す暗号化装置２０と、図５に示す復号装置３０との構成と同じである。但し、各構成要素で入出力される情報が異なる。

[0078] ＊＊＊動作の説明＊＊＊

図１６から図１８と、図６から図１０とを参照して、実施の形態２に係る暗号システム１の動作を説明する。

実施の形態２に係る暗号システム１の動作は、実施の形態２に係る暗号方法に相当する。また、実施の形態２に係る暗号システム１の動作は、実施の形態２に係る暗号プログラムの処理に相当する。

[0079] 図１６及び図６を参照して、実施の形態２に係るＳｅｔｕｐアルゴリズムを説明する。

Ｓｅｔｕｐアルゴリズムは、鍵生成装置１０によって実行される。

[0080] （ステップＳ１１：ＩＰＧ生成処理）

マスター鍵生成部１４は、入出力インタフェース１３を介してセキュリティパラメータ$１^{λ}$の入力を受け付ける。マスター鍵生成部１４は、受け付けられたセキュリティパラメータ$１^{λ}$と、１以上の整数ｄとを入力として、ＩＰＧ生成アルゴリズム$Ｇｅｎ^{IPG}（１^{λ}，ｄ）$を実行して、数１１５に示す公開パラメータ$ｐｋ^{IPG}$とマスター秘密鍵$ｓｋ^{IPG}$とのマスター鍵ペアを生成する。

[数115]

$$(\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_t, \hat{\mathbb{G}}_t, g_t, \hat{g}_t, e_t)_{t\in[0,d]}, \mathbb{G}_T)),\ \mathrm{sk}^{\mathrm{IPG}} := (\phi_t)_{t\in[d]}) \xleftarrow{R} \mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda}, d)$$

[0081] つまり、図１に示すように、実施の形態１では、ｔ＝０，１，．．．．，ｄについての群G_t及び群$\hat{G}_t$とペアリング演算e_tと、群G_Tと、ｔ＝１，．．．，ｄについての同種写像ϕ_tとが生成される。つまり、ｄ＋１個のペアリング群が用いられる。

ここで、ｔ＝１，．．．，ｄの群G_t及び群$\hat{G}_t$に属性が設定される。したがって、整数ｄの値は、設定したい属性の数に応じて決定される。

[0082] （ステップＳ１２：ハッシュ関数生成処理）

実施の形態１と同様に、マスター鍵生成部１４は、ハッシュ関数Ｈを生成する。

[0083] （ステップＳ１３：マスター鍵生成処理）

マスター鍵生成部１４は、ステップＳ１１で生成された公開パラメータpk^{IPG}と、ステップＳ１２で生成されたハッシュ関数Ｈとを用いて、公開パラメータ$pk:=((G_t, \hat{G}_t, g_t, e_t)_{t\in[0,d]}, G_T, H)$を生成する。鍵出力部１６は、公開パラメータｐｋを入出力インタフェース１３を介して外部の公開用サーバ等へ出力することにより、公開パラメータｐｋを暗号化装置２０及び復号装置３０に出力する。

また、マスター鍵生成部１４は、ステップＳ１１で生成されたマスター秘密鍵sk^{IPG}を用いて、マスター秘密鍵$sk:=(\phi_t)_{t\in[d]}$を生成する。マスター鍵生成部１４は、生成されたマスター秘密鍵ｓｋを記憶装置１２に書き込む。

[0084] つまり、マスター鍵生成部１４は、数１１６に示すＳｅｔｕｐアルゴリズムを実行して、マスター鍵ペアを生成する。

[数116]

$$\begin{aligned}&\mathrm{Setup}(1^\lambda):\\&(\mathrm{pk}^{\mathrm{IPG}}:=((\mathbb{G}_t,\hat{\mathbb{G}}_t,g_t,\hat{g}_t,e_t)_{t\in[0,d]},\mathbb{G}_T)),\ \mathrm{sk}^{\mathrm{IPG}}:=(\phi_t)_{t\in[d]})\\&\qquad\qquad\xleftarrow{\mathrm{R}}\mathrm{Gen}^{\mathrm{IPG}}(1^\lambda,d),\\&\text{generate a random hash } H:\mathbb{F}_q\to\mathbb{G}_0 \text{ with the identity space } \mathbb{F}_q,\\&\text{return pk}:=((\mathbb{G}_t,\hat{\mathbb{G}}_t,\hat{g}_t,e_t)_{t\in[0,d]},\mathbb{G}_T,H),\ \mathrm{sk}:=(\phi_t)_{t\in[d]}.\end{aligned}$$

[0085] 図１６及び図８を参照して、実施の形態２に係るＫｅｙＧｅｎアルゴリズムを説明する。

ＫｅｙＧｅｎアルゴリズムは、鍵生成装置１０によって実行される。

[0086] （ステップＳ２１：ＩＤ受付処理）

復号鍵生成部１５は、入出力インタフェース１３を介して、復号鍵$sk_{tag,S}$を使用するユーザの入力タグｔａｇ及びアクセスストラクチャＳ：＝（Ｍ，ρ）の入力を受け付ける。アクセスストラクチャＳは、復号鍵$sk_{tag,S}$で復号可能な範囲を示すものである。

[0087] （ステップＳ２２：鍵要素生成処理）

復号鍵生成部１５は、ステップＳ２１で受け付けられた入力タグｔａｇを入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈを計算して、群G_0の要素である要素h_0を生成する。

復号鍵生成部１５は、$1^{\rightarrow}\cdot u^{\rightarrow}=1$であるベクトル$u^{\rightarrow}$をランダムに選択する。復号鍵生成部１５は、ｉ∈［Ｌ］に対して、$s_i:=M_i\cdot u^{\rightarrow}$とし、ｔ：＝ρ（ｉ）として、数１１７に示すように、マスター秘密鍵ｓｋに含まれる同種写像ϕ_tで要素h_0を変換して、要素k_iを生成する。

[数117]

$$k_i := \phi_t(h_0)^{s_i}$$

[0088] （ステップＳ２３：鍵要素出力処理）

鍵出力部１６は、ステップＳ２１で受け付けられた入力タグｔａｇ及びアクセスストラクチャＳと、ステップＳ２２で生成されたｉ∈［Ｌ］についての要素k_iとを鍵要素とする復号鍵$sk_{tag,S}$を、入出力インタフェース１３を介して復号装置３０に出力する。この際、鍵出力部１６は、何らかの暗号方式で暗号化するといった方法により、復号鍵$sk_{tag,S}$が第三者に漏えいしないようにする。

[0089] つまり、復号鍵生成部１５は、数１１８に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵$sk_{tag,S}$を生成する。

[数118]

$$\begin{aligned}&\mathrm{KeyGen(pk,sk,tag,}\mathbb{S}:=(M,\rho)):\\&h_0:=H(\mathrm{tag})\in\mathbb{G}_0,\\&\text{choose random }\vec{u}\text{ such that }\vec{1}\cdot\vec{u}=1,\\&\text{for } i\in[L],\ s_i:=M_i\cdot\vec{u},\ t:=\rho(i),\ k_i:=\phi_t(h_0)^{s_i},\\&\text{return } \mathrm{sk}_{\mathrm{tag},\mathbb{S}}:=(\mathrm{tag},\ \mathbb{S},\ \{k_i\}_{i\in[L]}).\end{aligned}$$

[0090] 図１７及び図９を参照して、実施の形態２に係るＥｎｃアルゴリズムを説明する。

Ｅｎｃアルゴリズムは、暗号化装置２０によって実行される。

[0091] （ステップＳ３１：入力受付処理）

入力受付部２４は、入出力インタフェース２３を介して、鍵生成装置１０によって生成された公開パラメータｐｋと、暗号化対象のメッセージｍと、復号条件となる入力タグｔａｇ’及び属性集合Γとの入力を受け付ける。

[0092] （ステップＳ３２：暗号文生成処理）

暗号文生成部２５は、ステップＳ３１で受け付けられた入力タグｔａｇ’を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈを計算して、群G_0の要素である要素h_0を生成する。また、暗号文生成部２５は、一様乱数ζを生成する。

暗号文生成部２５は、属性集合Γに含まれる各整数ｔについて、一様乱数ζを用いて、数１１９に示す要素c_tを生成する。

[数119]

$$c_t:=\hat{g}_t^{\zeta}$$

また、暗号文生成部２５は、要素h_0及び一様乱数ζを用いて、数１２０に示す要素ｚを生成する。そして、暗号文生成部２５は、ステップＳ３１で受け付けられたメッセージｍと、要素ｚを用いて要素$c_T:=z\cdot m$を生成する。

[数120]

$$z := e_0(h_0, \hat{g}_0)^{\zeta}$$

[0093] （ステップＳ３３：暗号文出力処理）

暗号文出力部２６は、ステップＳ３１で受け付けられた入力タグｔａｇ’及び属性集合Γと、ステップＳ３２で生成された属性集合Γに含まれる各整数ｔについての要素c_t及び要素c_Tとを暗号要素とする暗号文$ct_{tag',\Gamma}$を、入出力インタフェース２３を介して復号装置３０に出力する。

[0094] つまり、暗号化装置２０は、数１２１に示すＥｎｃアルゴリズムを実行して、暗号文$ct_{tag',\Gamma}$を生成する。

[数121]

$$\begin{aligned}&\mathrm{Enc}(\mathrm{pk}, m, \mathrm{tag}', \Gamma):\\ &h_0 := H(\mathrm{tag}') \in \mathbb{G}_0,\ \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q,\\ &\text{for } t \in \Gamma,\ c_t := \hat{g}_t^{\zeta},\ z := e_0(h_0, \hat{g}_0)^{\zeta},\ c_T := z \cdot m,\\ &\text{return } \mathrm{ct}_{\mathrm{tag}',\Gamma} := (\mathrm{tag}', \Gamma, \{c_t\}_{t\in\Gamma}, c_T).\end{aligned}$$

[0095] 図１８及び図１０を参照して、実施の形態２に係るＤｅｃアルゴリズムを説明する。

Ｄｅｃアルゴリズムは、復号装置３０によって実行される。

[0096] （ステップＳ４１：入力受付処理）

入力受付部３４は、入出力インタフェース３３を介して、鍵生成装置１０によって生成された公開パラメータｐｋ及び復号鍵$sk_{tag,S}$と、暗号化装置２０によって生成された暗号文$ct_{tag',\Gamma}$との入力を受け付ける。

[0097] （ステップＳ４２：復号判定処理）

復号部３５は、ステップＳ４１で受け付けられた復号鍵$sk_{tag,S}$に含まれる入力タグｔａｇと、暗号文$ct_{tag',\Gamma}$に含まれる入力タグｔａｇ’とが等しいか否かを判定する。また、復号部３５は、復号鍵$sk_{tag,S}$に含まれるアクセスストラクチャＳが、暗号文$ct_{tag',\Gamma}$に含まれる属性集合Γを受理するか否かを判定する。これにより、暗号文$ct_{tag',\Gamma}$を復号鍵$sk_{tag,S}$で

復号可能かが判定される。

復号部３５は、入力タグｔａｇと入力タグｔａｇ’とが等しいと判定され、かつ、アクセスストラクチャＳが属性集合Γを受理すると判定された場合、処理をステップＳ４３に進め、そうでない場合、処理をステップＳ４５に進める。

[0098] （ステップＳ４３：復号処理）

復号部３５は、ρ（ｉ）∈Γについて、数１２２を満たす補完係数α_iを計算する。なお、M_iは、行列Ｍのｉ行目である。

[数122]

$$\vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i$$

復号部３５は、計算された補完係数α_iを用いて、ステップＳ４１で受け付けられた復号鍵$sk_{tag,S}$に含まれる要素k_iと、暗号文$ct_{tag',\Gamma}$に含まれる暗号要素c_tとについて数１２３に示すペアリング演算を行い、要素ｚ’を計算する。

[数123]

$$z' = \prod_{t:=\rho(i)\in\Gamma} e_t(k_i, c_t)^{\sigma_i}$$

復号部３５は、計算された要素ｚ’を用いて、メッセージｍ’：＝c_T・（ｚ’）$^{-1}$を計算する。

[0099] ステップＳ４４からステップＳ４５の処理は、実施の形態１と同じである。

[0100] つまり、復号装置３０は、数１２４に示すＤｅｃアルゴリズムを実行して、暗号文$ct_{ID'}$を復号鍵sk_{ID}により復号する。

[数124]

$$\begin{aligned}&\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathrm{tag},\mathbb{S}}, \mathrm{ct}_{\mathrm{tag}',\Gamma}):\\&\quad \text{if } (\mathrm{tag} = \mathrm{tag}') \text{ and } \mathbb{S} \text{ accepts } \Gamma,\\&\qquad \text{then compute}\\&\qquad\quad \{\sigma_i\}_{\rho(i)\in\Gamma} \text{ such that } \vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i\\&\qquad\quad \text{where } M_i \text{ is the } i\text{-th row of } M,\\&\qquad z' = \prod_{t:=\rho(i)\in\Gamma} e_t(k_i, c_t)^{\sigma_i},\ m' := c_T \cdot (z')^{-1},\\&\qquad \text{return } m'.\\&\quad \text{otherwise, return } \perp.\end{aligned}$$

[0101] 数１２５に示すように、ステップＳ４３で暗号文ｃｔ$_{\mathrm{tag}',\Gamma}$を復号鍵ｓｋ$_{\mathrm{tag},\mathbb{S}}$で復号可能である。

[数125]

$$\begin{aligned}z' &= \prod_{t:=\rho(i)\in\Gamma} e_t(k_i, c_t)^{\sigma_i}\\&= \prod_{t:=\rho(i)\in\Gamma} e_t(\phi_t(h_0)^{s_i}, \hat{g}_t^{\zeta})^{\sigma_i}\\&= \prod_{t:=\rho(i)\in\Gamma} e_t(\phi_t(h_0), \hat{g}_t)^{\zeta\sigma_i s_i}\\&= \prod_{t:=\rho(i)\in\Gamma} e_0(h_0, \hat{g}_0)^{\zeta\sigma_i s_i}\\&= \prod_{t:=\rho(i)\in\Gamma} e_0(h_0, \hat{g}_0)^{\zeta}\\&= z\end{aligned}$$

[0102] ＊＊＊実施の形態２の効果＊＊＊

以上のように、実施の形態２に係る暗号システム１は、ＩＰＧを用いてＡＢＥ方式を実現する。ここで、鍵生成装置１０によって生成されるマスター秘密鍵ｓｋ：＝ϕ_tは、実施の形態１と同様に耐量子性を有している。そのため、量子計算機によってでも、マスター秘密鍵ｓｋが破られることがない。

[0103] 実施の形態３．

実施の形態３では、どの部分ユニバース識別子ｔについても属性x_t：＝（$x_{t,j}$）$_{j\in[n]}$がユニバースＵ：＝｛０，１｝^{n}の要素である場合におけるＡＢＥ方式につい

て説明する。実施の形態３では、実施の形態２と異なる点を説明する。

[0104] 実施の形態３では、ＡＢＥの小さなユニバースの２つのインスタンスｔ∈［ｄ］及びｊ∈［ｎ］についての階層的な構造が用いられる。そして、実施の形態３では、下位の階層のインスタンスにおいて、ｎ－ｏｕｔ－ｏｆ－２ｎの秘密共有述語の特別な形態が、長さｎの２値の識別子x_tに対する識別子マッチングに用いられる。

[0105] ＊＊＊動作の説明＊＊＊

図１６から図１８と、図６から図１０とを参照して、実施の形態３に係る暗号システム１の動作を説明する。

実施の形態３に係る暗号システム１の動作は、実施の形態３に係る暗号方法に相当する。また、実施の形態３に係る暗号システム１の動作は、実施の形態３に係る暗号プログラムの処理に相当する。

[0106] 図１６及び図６を参照して、実施の形態３に係るＳｅｔｕｐアルゴリズムを説明する。

Ｓｅｔｕｐアルゴリズムは、鍵生成装置１０によって実行される。

[0107] （ステップＳ１１：ＩＰＧ生成処理）

マスター鍵生成部１４は、入出力インタフェース１３を介してセキュリティパラメータ1^λの入力を受け付ける。マスター鍵生成部１４は、受け付けられたセキュリティパラメータ1^λと、１以上の整数ｄ及び１以上の整数ｎについての整数２ｄｎとを入力として、ＩＰＧ生成アルゴリズムGen^{IPG}（1^λ，２ｄｎ）を実行して、数１２６に示す公開パラメータpk^{IPG}とマスター秘密鍵sk^{IPG}とのマスター鍵ペアを生成する。

[数126]

$$(\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_0, \hat{\mathbb{G}}_0, g_0, \hat{g}_0, e_0),$$
$$(\mathbb{G}_{t,j,\iota}, \hat{\mathbb{G}}_{t,j,\iota}, g_{t,j,\iota}, \hat{g}_{t,j,\iota}, e_{t,j,\iota})_{\iota\in[0,1]}^{t\in[d],j\in[n]}, \mathbb{G}_T)),$$
$$\mathrm{sk}^{\mathrm{IPG}} := (\phi_{t,j,\iota})_{\iota\in[0,1]}^{t\in[d],j\in[n]})$$
$$\xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda}, d)$$

[0108] つまり、実施の形態１では、ｔ＝０，１，．．．，ｄとｊ＝１，．．．，ｎとι＝０，１とについての群$G_{t,j,\iota}$及び群$\hat{G}_{t,j,\iota}$とペアリング演算e_tと、群G_Tと、ｔ＝１，．．．，ｄとｊ＝１，．．．，ｎとι＝０，１とについての同種写像$\phi_{t,j,\iota}$とが生成される。つまり、２ｄｎ＋１個のペアリング群が用いられる。

ここで、ｔ＝１，．．．，ｄとｊ＝１，．．．，ｎとι＝０，１の群$G_{t,j,\iota}$及び群$\hat{G}_{t,j,\iota}$に属性が設定される。したがって、整数ｄ，ｎの値は、設定したい属性の数に応じて決定される。

[0109] （ステップＳ１２：ハッシュ関数生成処理）

実施の形態１と同様に、マスター鍵生成部１４は、ハッシュ関数Ｈを生成する。

[0110] （ステップＳ１３：マスター鍵生成処理）

マスター鍵生成部１４は、ステップＳ１１で生成された公開パラメータ$\mathrm{pk}^{\mathrm{IPG}}$と、ステップＳ１２で生成されたハッシュ関数Ｈとを用いて、公開パラメータｐｋ：＝（$(G_t, \hat{G}_t, g_t, e_t)_{t\in[0,d],j\in[n],\iota\in[0,1]}$, G_T, Ｈ）を生成する。鍵出力部１６は、公開パラメータｐｋを入出力インタフェース１３を介して

外部の公開用サーバ等へ出力することにより、公開パラメータｐｋを暗号化装置２０及び復号装置３０に出力する。

また、マスター鍵生成部１４は、ステップＳ１１で生成されたマスター秘密鍵$\mathrm{sk}^{\mathrm{IPG}}$を用いて、マスター秘密鍵ｓｋ：＝$(\phi_{t,j,\iota})_{t\in[d],j\in[n],\iota\in[0,1]}$を生成する。マスター鍵生成部１４は、生成されたマスター秘密鍵

ｓｋを記憶装置１２に書き込む。

[0111] つまり、マスター鍵生成部１４は、数１２７に示すＳｅｔｕｐアルゴリズムを実行して、マスター鍵ペアを生成する。

[数127]

$$\begin{aligned}
&\mathrm{Setup}(1^{\lambda}):\\
&(\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_0,\hat{\mathbb{G}}_0,g_0,\hat{g}_0,e_0),\\
&\qquad (\mathbb{G}_{t,j,\iota},\hat{\mathbb{G}}_{t,j,\iota},g_{t,j,\iota},\hat{g}_{t,j,\iota},e_{t,j,\iota})_{\iota\in[0,1]}^{t\in[d],j\in[n]},\mathbb{G}_T)),\\
&\mathrm{sk}^{\mathrm{IPG}} := (\phi_{t,j,\iota})_{\iota\in[0,1]}^{t\in[d],j\in[n]})\\
&\qquad \xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda},d),\\
&\text{generate a random hash } H:\mathbb{F}_q\to\mathbb{G}_0 \text{ with the identity space } \mathbb{F}_q,\\
&\text{return pk} := ((\mathbb{G}_0,\hat{\mathbb{G}}_0,\hat{g}_0,e_0),(\mathbb{G}_{t,j,\iota},\hat{\mathbb{G}}_{t,j,\iota},\hat{g}_{t,j,\iota},e_{t,j,\iota})_{\iota\in[0,1]}^{t\in[d],j\in[n]},\\
&\qquad \mathbb{G}_T,H),\\
&\mathrm{sk} := (\phi_{t,j,\iota})_{\iota\in[0,1]}^{t\in[d],j\in[n]}.
\end{aligned}$$

[0112] 図１６及び図８を参照して、実施の形態２に係るＫｅｙＧｅｎアルゴリズムを説明する。

ＫｅｙＧｅｎアルゴリズムは、鍵生成装置１０によって実行される。

[0113] ステップＳ２１の処理は、実施の形態２と同じである。

[0114] （ステップＳ２２：鍵要素生成処理）

復号鍵生成部１５は、ステップＳ２１で受け付けられた入力タグｔａｇを入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈを計算して、群G_0の要素である要素h_0を生成する。

復号鍵生成部１５は、$1^{\rightarrow}\cdot u^{\rightarrow}=1$であるベクトル$u^{\rightarrow}$をランダムに選択する。復号鍵生成部１５は、$i\in[L]$に対して、$s_i:=M_i\cdot u^{\rightarrow}$とし、$s_i=\Sigma_{j=1}^{n}\tau_{i,j}$である乱数$\tau^{\rightarrow}:=(\tau_{i,j})$を選択する。復号鍵生成部１５は、乱数$\tau^{\rightarrow}$を用いて、数１２８に示すように、マスター秘密鍵ｓｋに含まれる同種写像$\phi_{t,j,\iota}$で要素h_0を変換して、要素$k_{i,j}$を生成する。

[数128]

$$\text{if } \rho(i) = (t, v_i := (v_{i,j}) \in \{0,1\}^n),$$
$$k_{i,j} := \phi_{t,j,v_{i,j}}(h_0)^{\tau_{i,j}}$$

[0115] （ステップＳ２３：鍵要素出力処理）

鍵出力部１６は、ステップＳ２１で受け付けられた入力タグｔａｇ及びアクセスストラクチャＳと、ステップＳ２２で生成されたｉ∈［Ｌ］及びｊ∈［ｎ］についての要素$k_{i,j}$とを鍵要素とする復号鍵$sk_{tag,S}$を、入出力インタフェース１３を介して復号装置３０に出力する。この際、鍵出力部１６は、何らかの暗号方式で暗号化するといった方法により、復号鍵$sk_{tag,S}$が第三者に漏えいしないようにする。

[0116] つまり、復号鍵生成部１５は、数１２９に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵$sk_{tag,S}$を生成する。

[数129]

$$\text{KeyGen(pk,sk,tag,}\mathbb{S} := (M, \rho)):$$
$$h_0 := H(\text{tag}) \in \mathbb{G}_0,$$
$$\text{choose random } \vec{u} \text{ such that } \vec{1} \cdot \vec{u} = 1,$$
$$\text{for } i \in [L],$$
$$s_i := M_i \cdot \vec{u},$$
$$\text{choose random } \vec{\tau_i} := (\tau_{i,j}) \text{ such that } s_i := \sum_{j=1}^{n} \tau_{i,j},$$
$$\text{if } \rho(i) = (t, v_i := (v_{i,j}) \in \{0,1\}^n),$$
$$k_{i,j} := \phi_{t,j,v_{i,j}}(h_0)^{\tau_{i,j}},$$
$$\text{return } \text{sk}_{\text{tag},\mathbb{S}} := (\text{tag}, \mathbb{S}, \{k_{i,j}\}_{i \in [L], j \in [n]}).$$

[0117] 図１７及び図９を参照して、実施の形態２に係るＥｎｃアルゴリズムを説明する。

Ｅｎｃアルゴリズムは、暗号化装置２０によって実行される。

[0118] ステップＳ３１の処理は、実施の形態２と同じである。

[0119] （ステップＳ３２：暗号文生成処理）

暗号文生成部２５は、ステップＳ３１で受け付けられた入力タグｔａｇ’を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈを計算して、群G_0の要素である要素h_0を生成する。また、暗号文生成部２５は、一様乱数ζを生成する。

暗号文生成部２５は、属性集合Γに含まれる（ｔ，$x_t := (x_{t,j}) \in \{0,1\}^n$）$\in \Gamma$の各整数ｔ及び各整数ｊについて、一様乱数$\zeta$を用いて、数１３０に示す要素$c_{t,j}$を生成する。

[数130]

$$c_{t,j} := \hat{g}_{t,j,x_{t,j}}^{\zeta}$$

また、暗号文生成部２５は、要素h_0及び一様乱数ζを用いて、数１３１に示す要素ｚを生成する。そして、暗号文生成部２５は、ステップＳ３１で受け付けられたメッセージｍと、要素ｚを用いて要素$c_T := z \cdot m$を生成する。

[数131]

$$z := e_0(h_0, \hat{g}_0)^{\zeta}$$

[0120] （ステップＳ３３：暗号文出力処理）

暗号文出力部２６は、ステップＳ３１で受け付けられた入力タグｔａｇ’及び属性集合Γと、ステップＳ３２で生成された属性集合Γに含まれる各整数ｔ及びｊ∈［ｎ］についての要素$c_{t,j}$及び要素c_Tとを暗号要素とする暗号文$ct_{tag',\Gamma}$を、入出力インタフェース２３を介して復号装置３０に出力する。

[0121] つまり、暗号化装置２０は、数１３２に示すＥｎｃアルゴリズムを実行して、暗号文$ct_{tag',\Gamma}$を生成する。

[数132]

$$\begin{aligned}&\mathrm{Enc}(\mathrm{pk}, m, \mathrm{tag}', \Gamma):\\&h_0 := H(\mathrm{tag}') \in \mathbb{G}_0,\ \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q,\\&\text{for } (t, x_t := (x_{i,j}) \in \{0,1\}^n) \in \Gamma,\ c_{t,j} := \hat{g}_{t,j,x_{t,j}}^{\zeta},\\&z := e_0(h_0, \hat{g}_0)^{\zeta},\ c_T := z \cdot m,\\&\text{return } \mathrm{ct}_{\mathrm{tag}',\Gamma} := (\mathrm{tag}', \Gamma, \{c_{t,j}\}_{(t,\cdot)\in\Gamma, j\in[n]}, c_T).\end{aligned}$$

[0122] 図１８及び図１０を参照して、実施の形態２に係るＤｅｃアルゴリズムを説明する。

Ｄｅｃアルゴリズムは、復号装置３０によって実行される。

[0123] ステップＳ４１からステップＳ４２の処理は、実施の形態２と同じである。

[0124] （ステップＳ４３：復号処理）

復号部３５は、数１３３を満たす補完係数α_iを計算する。

[数133]

$$\vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i$$

復号部３５は、計算された補完係数α_iを用いて、ステップＳ４１で受け付けられた復号鍵$sk_{tag,S}$に含まれる要素$k_{i,j}$と、暗号文$ct_{tag',\Gamma}$に含まれる暗号要素$c_{t,j}$とについて数１３４に示すペアリング演算を行い、要素ｚ’を計算する。

[数134]

$$z' = \prod_{\rho(i)=(t,(v_{i,j}))\in\Gamma} \left(\prod_{j=1}^{n} e_{t,j,v_{i,j}}(k_{i,j}, c_{t,j}) \right)^{\sigma_i}$$

復号部３５は、計算された要素ｚ’を用いて、メッセージｍ’：＝c_T・（ｚ’）$^{-1}$を計算する。

[0125] ステップＳ４４からステップＳ４５の処理は、実施の形態２と同じである

。

[0126] つまり、復号装置３０は、数１３５に示すＤｅｃアルゴリズムを実行して、暗号文$ct_{ID'}$を復号鍵sk_{ID}により復号する。

[数135]

$$\begin{aligned}&\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathrm{tag},\mathbb{S}}, \mathrm{ct}_{\mathrm{tag}',\Gamma}):\\&\text{if } (\mathrm{tag} = \mathrm{tag}') \text{ and } \mathbb{S} \text{ accepts } \Gamma,\\&\quad \text{then compute}\\&\quad \{\sigma_i\}_{\rho(i)\in\Gamma} \text{ such that } \vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i\\&\quad \text{where } M_i \text{ is the } i\text{-th row of } M,\\&z' = \prod_{\rho(i)=(t,(v_{i,j}))\in\Gamma}\left(\prod_{j=1}^{n} e_{t,j,v_{i,j}}(k_{i,j}, c_{t,j})\right)^{\sigma_i},\\&m' := c_T \cdot (z')^{-1},\\&\quad \text{return } m'.\\&\text{otherwise, return } \perp.\end{aligned}$$

[0127] 数１３６に示すように、ステップＳ４３で暗号文$ct_{tag',\Gamma}$を復号鍵$sk_{tag,\mathbb{S}}$で復号可能である。

[数136]

$$\begin{aligned}z' &= \prod_{\rho(i)=(t,(v_{i,j}))\in\Gamma}\left(\prod_{j=1}^{n} e_{t,j,v_{i,j}}(k_{i,j}, c_{t,j})\right)^{\sigma_i}\\&= \prod_{\rho(i)=(t,(v_{i,j}))\in\Gamma}\left(\prod_{j=1}^{n} e_{t,j,v_{i,j}}(\phi_{t,j,v_{i,j}}(h_0)^{\tau_{i,j}}, \hat{g}_{t,j,v_{i,j}}^{\zeta})\right)^{\sigma_i}\\&= \prod_{\rho(i)=(t,\cdot)\in\Gamma}\left(\prod_{j=1}^{n} e_0(h_0, \hat{g}_0)^{\zeta\tau_{i,j}}\right)^{\sigma_i}\\&= \prod_{\rho(i)=(t,\cdot)\in\Gamma}\left(e_0(h_0, \hat{g}_0)^{\zeta s_i}\right)^{\sigma_i}\\&= z\end{aligned}$$

[0128] ＊＊＊実施の形態３の効果＊＊＊

以上のように、実施の形態３に係る暗号システム１は、ＩＰＧを用いて大きいユニバースについてのＡＢＥ方式を実現する。ここで、鍵生成装置１０によって生成されるマスター秘密鍵ｓｋ：＝ϕ_tは、実施の形態２と同様に耐量子性を有している。そのため、量子計算機によってでも、マスター秘密鍵ｓｋが破られることがない。

[0129] 実施の形態４.

実施の形態４では、階層的なＩＢＥ（以下、ＨＩＢＥ）方式について説明する。実施の形態４では、実施の形態１と異なる点を説明する。

[0130] ＊＊＊動作の説明＊＊＊

図３から図９を参照して、実施の形態４に係る暗号システム１の動作を説明する。

実施の形態４に係る暗号システム１の動作は、実施の形態４に係る暗号方法に相当する。また、実施の形態４に係る暗号システム１の動作は、実施の形態４に係る暗号プログラムの処理に相当する。

[0131] 図３及び図６を参照して、実施の形態１に係るＳｅｔｕｐアルゴリズムを説明する。

Ｓｅｔｕｐアルゴリズムは、鍵生成装置１０によって実行される。

[0132] ステップＳ１１の処理は、実施の形態１と同じである。

[0133] （ステップＳ１２：ハッシュ関数生成処理）

マスター鍵生成部１４は、ｔ＝０，１について、識別子の空間である体F_qの要素を、群G_tの要素に変換するランダムなハッシュ関数H_tを生成する。

[0134] （ステップＳ１３：マスター鍵生成処理）

マスター鍵生成部１４は、ステップＳ１１で生成された公開パラメータpk^{IPG}と、ステップＳ１２で生成されたハッシュ関数Ｈとを用いて、公開パラメータｐｋ：＝（（G_t，$\hat{G}_t$，$\hat{g}_t$，e_t，H_t）$_{t=0,1}$，G_T）を生成する。鍵出力部１６は、公開パラメータｐｋを入出力インタフェース１３を介して外部の公開用サー

バ等へ出力することにより、公開パラメータｐｋを暗号化装置２０及び復号装置３０に出力する。

また、マスター鍵生成部１４は、ステップＳ１１で生成されたマスター秘密鍵ｓｋ$_{IPG}$を用いて、マスター秘密鍵ｓｋ：＝ϕ_1を生成する。マスター鍵生成部１４は、生成されたマスター秘密鍵ｓｋを記憶装置１２に書き込む。

[0135] つまり、マスター鍵生成部１４は、数１３７に示すＳｅｔｕｐアルゴリズムを実行して、マスター鍵ペアを生成する。

[数137]

$$\begin{aligned}&\mathrm{Setup}(1^{\lambda}):\\&(\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_t,\hat{\mathbb{G}}_t,g_t,\hat{g}_t,e_t)_{t=0,1},\mathbb{G}_T)),\ \mathrm{sk}^{\mathrm{IPG}} := \phi_1)\\&\qquad\qquad \xleftarrow{\mathrm{R}} \mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda},1),\\&\text{generate a random hash } H_t : \mathbb{F}_q \to \mathbb{G}_0 \text{ with the identity space } \mathbb{F}_q,\\&\text{return pk} := ((\mathbb{G}_t,\hat{\mathbb{G}}_t,\hat{g}_t,e_t,H_t)_{t=0,1},\mathbb{G}_T),\ \mathrm{sk} := \phi_1.\end{aligned}$$

[0136] 図３及び図８を参照して、実施の形態４に係るＫｅｙＧｅｎアルゴリズムを説明する。

ＫｅｙＧｅｎアルゴリズムは、鍵生成装置１０によって実行される。

[0137] （ステップＳ２１：ＩＤ受付処理）

復号鍵生成部１５は、入出力インタフェース１３を介して、復号鍵ｓｋ$_{ID}$を使用するユーザの識別子ＩＤの入力を受け付ける。ここでは、識別子ＩＤは、ｉ∈［ｊ］についてのＩＤ$_i$から構成される。ｊは、２以上の整数である。

[0138] （ステップＳ２２：鍵要素生成処理）

復号鍵生成部１５は、ｉ∈［ｊ－１］について、数１３８に示すように、要素ｄ＾$_i$を生成する。

[数138]

$$\begin{aligned}&r_i \xleftarrow{\mathrm{U}} \mathbb{F}_q,\\&\hat{d}_i := \hat{g}_1^{r_i} \in \hat{\mathbb{G}}_1\end{aligned}$$

復号鍵生成部１５は、ステップＳ２１で受け付けられた識別子ＩＤを構成するＩＤ$_1$を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈ$_0$を計算して、群Ｇ$_0$の要素である要素ｈ$_1$を生成する。また、復号鍵生成部１５は、ｉ∈［２，ｊ］について、識別子ＩＤを構成するＩＤ$_1$，．．．，ＩＤ$_i$を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈ$_1$を計算して、群Ｇ$_1$の要素である要素ｈ$_i$を生成する。そして、復号鍵生成部１５は、数１３９に示すように、マスター秘密鍵ｓｋに含まれる同種写像ϕ_1で要素ｈ$_1$を変換した要素ｄ$_j$を生成する。

[数139]

$$d_j := \phi_1(h_1) \cdot \prod_{i=2}^{j} h_i^{r_{i-1}}$$

[0139] （ステップＳ２３：鍵要素出力処理）

鍵出力部１６は、ステップＳ２１で受け付けられた識別子ＩＤと、ステップＳ２２で生成された、ｉ∈［ｊ－１］についての要素ｄ＾$_j$及び要素ｄ$_j$とを鍵要素とする復号鍵ｓｋ$_{ID}$を、入出力インタフェース１３を介して復号装置３０に出力する。この際、鍵出力部１６は、何らかの暗号方式で暗号化するといった方法により、復号鍵ｓｋ$_{ID}$が第三者に漏えいしないようにする。

[0140] つまり、復号鍵生成部１５は、数１４０に示すＫｅｙＧｅｎアルゴリズムを実行して、復号鍵ｓｋ$_{ID}$を生成する。

[数140]

$$\begin{aligned}
&\mathrm{KeyGen}(\mathrm{pk}, \mathrm{sk}, (\mathrm{ID}_i)_{i\in[j]}):\\
&\quad \text{for } i\in[j-1],\\
&\quad\quad r_i \xleftarrow{\mathrm{U}} \mathbb{F}_q,\ \hat{d}_i := \hat{g}_1^{r_i} \in \hat{\mathbb{G}}_1\\
&\quad h_1 := H_0(\mathrm{ID}_1) \in \mathbb{G}_0,\\
&\quad \text{for } i\in[2,j],\\
&\quad\quad h_i := H_1(\mathrm{ID}_1,...,\mathrm{ID}_i) \in \mathbb{G}_1,\\
&\quad d_j := \phi_1(h_1)\cdot\prod_{i=2}^{j} h_i^{r_{i-1}}\\
&\quad \text{return } \mathrm{sk}_{\mathrm{ID}} := ((\mathrm{ID}_i)_{i\in[j]}, (\hat{d}_i\in\hat{\mathbb{G}}_1)_{i\in[j-1]}, d_j\in\mathbb{G}_1).
\end{aligned}$$

[0141] 図４及び図９を参照して、実施の形態１に係るＥｎｃアルゴリズムを説明する。

Ｅｎｃアルゴリズムは、暗号化装置２０によって実行される。

[0142] （ステップＳ３１：入力受付処理）

入力受付部２４は、入出力インタフェース２３を介して、鍵生成装置１０によって生成された公開パラメータｐｋと、暗号化対象のメッセージｍと、復号条件となる識別子ＩＤ’との入力を受け付ける。ここでは、識別子ＩＤ’は、ｉ∈［ｊ］についてのＩＤ’$_i$から構成される。

[0143] （ステップＳ３２：暗号文生成処理）

暗号文生成部２５は、一様乱数ζを生成する。暗号文生成部２５は、一様乱数ζを用いて、数１４１に示す要素ｃ＾$_0$を生成する。

[数141]

$$\hat{c}_0 := \hat{g}_1^{\zeta}$$

暗号文生成部２５は、ｉ∈［２，ｊ］について、識別子ＩＤを構成するＩＤ’$_1$，．．．，ＩＤ’$_i$を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈ$_1$を計算して、群Ｇ$_1$の要素である要素ｈ$_i$を生成する。暗号文生成部２５は、要素ｈ$_i$を用いて、数１４２に示す要素ｃ$_i$を生成する。

[数142]

$$c_i := h_i^{\zeta}$$

暗号文生成部２５は、ステップＳ３１で受け付けられた識別子ＩＤ’を構成するＩＤ’$_1$を入力として、公開パラメータｐｋに含まれるハッシュ関数Ｈ$_0$を計算して、群Ｇ$_0$の要素である要素ｈ$_1$を生成する。また、暗号文生成部２５は、要素ｈ$_1$及び一様乱数ζを用いて、数１４３に示す要素ｚを生成する。そして、暗号文生成部２５は、ステップＳ３１で受け付けられたメッセージｍと、要素ｚを用いて要素ｃ$_T$：＝ｚ・ｍを生成する。

[数143]

$$z := e_0(h_1, \hat{g}_0)^{\zeta}$$

[0144] （ステップＳ３３：暗号文出力処理）

暗号文出力部２６は、ステップＳ３１で受け付けられた識別子ＩＤ’と、ステップＳ３２で生成された要素ｃ^$_0$，（ｃ$_i$）$_{i\in[2,\ j]}$，ｃ$_T$とを暗号要素とする暗号文ｃｔ$_{ID'}$を、入出力インタフェース２３を介して復号装置３０に出力する。

[0145] つまり、暗号化装置２０は、数１４４に示すＥｎｃアルゴリズムを実行して、暗号文ｃｔ$_{ID'}$を生成する。

[数144]

$$\begin{aligned}
&\mathrm{Enc}(\mathrm{pk}, m, (\mathrm{ID}'_i)_{i\in[j]}):\\
&\zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\times},\ \hat{c}_0 := \hat{g}_1^{\zeta},\\
&\text{for } i \in [2, j],\\
&\quad h_i := H_1(\mathrm{ID}'_1, \ldots, \mathrm{ID}'_i) \in \mathbb{G}_1,\ c_i := h_i^{\zeta},\\
&h_1 := H_0(\mathrm{ID}'_1) \in \mathbb{G}_0,\ z := e_0(h_1, \hat{g}_0)^{\zeta},\ c_T := z \cdot m,\\
&\text{return } \mathrm{ct}_{\mathrm{ID}'} := ((\mathrm{ID}'_i)_{i\in[j]},\ \hat{c}_0 \in \hat{\mathbb{G}}_1,\ (c_i \in \hat{\mathbb{G}}_1)_{i\in[2,j]},\ c_T).
\end{aligned}$$

[0146] 図５及び図１０を参照して、実施の形態１に係るＤｅｃアルゴリズムを説明する。

Ｄｅｃアルゴリズムは、復号装置３０によって実行される。

[0147] ステップＳ４１からステップＳ４２の処理は、実施の形態１と同じである。

[0148] （ステップＳ４３：復号処理）

復号部３５は、ステップＳ４１で受け付けられた復号鍵sk_{ID}に含まれる要素$\hat{d}_j$及び要素d_jと、暗号文$ct_{ID'}$に含まれる要素$\hat{c}_0$及び要素c_iとについて数１４５に示す演算を行い、要素ｚ’を計算する。復号部３５は、計算された要素ｚ’を用いて、メッセージｍ’：＝$c_T \cdot (z')^{-1}$を計算する。

[数145]

$$z' := \frac{e_1(d_j, \hat{c}_0)}{\prod_{i=2}^{j} e_1(c_i, \hat{d}_{i-1})}$$

[0149] ステップＳ４４からステップＳ４５の処理は、実施の形態１と同じである。

[0150] つまり、復号装置３０は、数１４６に示すＤｅｃアルゴリズムを実行して、暗号文$ct_{ID'}$を復号鍵sk_{ID}により復号する。

[数146]

$$\begin{aligned}
&\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathrm{ID}}, \mathrm{ct}_{\mathrm{ID}'}):\\
&\quad \text{if } (\mathrm{ID}_i = \mathrm{ID}'_i),\\
&\qquad z' := \frac{e_1(d_j, \hat{c}_0)}{\prod_{i=2}^{j} e_1(c_i, \hat{d}_{i-1})},\ m' := c_T \cdot (z')^{-1},\\
&\qquad \text{return } m'.\\
&\quad \text{otherwise, return } \perp.
\end{aligned}$$

[0151] 数１４７に示すように、ステップＳ４３で暗号文$ct_{tag',\Gamma}$を復号鍵$sk_{tag,S}$で復号可能である。

[数147]

$$z' := \frac{e_1(d_j, \hat{c}_0)}{\prod_{i=2}^{j} e_1(c_i, \hat{d}_{i-1})}$$
$$= \frac{e_1(\phi_1(h_1) \cdot \prod_{i=2}^{j} h_i^{r_{i-1}}, \hat{g}_1^{\zeta})}{\prod_{i=2}^{j} e_1(h_i^{\zeta}, \hat{g}_1^{r_{i-1}})}$$
$$= e_1(\phi_1(h_1) \cdot \hat{g}_1)^{\zeta}$$
$$= e_0(h_1 \cdot \hat{g}_0)^{\zeta}$$
$$= z$$

[0152] ＊＊＊実施の形態４の効果＊＊＊

以上のように、実施の形態４に係る暗号システム１は、ＩＰＧを用いてＨＩＢＥ方式を実現する。ここで、鍵生成装置１０によって生成されるマスター秘密鍵ｓｋ：＝ϕ_tは、実施の形態１と同様に耐量子性を有している。そのため、量子計算機によってでも、マスター秘密鍵ｓｋが破られることがない。

[0153] 実施の形態５.

実施の形態５では、ＩＰＧ生成アルゴリズムGen^{IPG}（1^{λ}，ｄ）について、楕円曲線を用いて具体的に説明する。

[0154] ＊＊＊動作の説明＊＊＊

図１９を参照して、実施の形態５に係るＩＰＧ生成アルゴリズムGen^{IPG}（1^{λ}，ｄ）の処理を説明する。

[0155] （ステップＳ５１：要素生成処理）

マスター鍵生成部１４は、十分に大きい、奇素数ｐについての超楕円曲線

E_0 / F_{p2}

（ここで、ｐ２はp^2）をランダムに生成する。

マスター鍵生成部１４は、適切な（Ｌ~，κ）と、楕円曲線E_0の部分群から構成される位数ｒの非対称ペアリング群（G_0，$\hat{G}_0$，G_T；e_0）を生成する。e_0は、楕円曲線E_0におけるヴェイユペアリング$e_{weil,0}$から、どの$h_0 \in G_0$及び$\hat{h}_0 \in \hat{G}_0$に対しても$e_0(h_0, \hat{h}_0) := e_{weil,0}(h$

$_0$，ｈ＾$_0$）$^{\Psi}$と定義される。Ψ＝（Ｌ~）$^{\kappa}$である。

マスター鍵生成部１４は、群Ｇ$_0$から要素ｇ$_0$を一様に選択し、群Ｇ＾$_0$から要素ｇ＾$_0$を一様に選択する。

[0156] （ステップＳ５２：同種生成処理）

マスター鍵生成部１４は、アルゴリズムＩｓｏｇ$_{L\sim,\kappa}$（Ｅ$_0$）を実行して、ｔ∈［ｄ］について、楕円曲線Ｅ$_0$と同種となる楕円曲線Ｅ$_t$と、楕円曲線Ｅ$_0$から楕円曲線Ｅ$_t$への同種写像を計算するためのトラップドアξ$_t$とをランダムに生成する。アルゴリズムＩｓｏｇ$_{L\sim,\kappa}$（Ｅ$_0$）として、図２０に示す非特許文献３に記載されたＩｓｏｇ$_{L\sim,\kappa}^{djp}$アルゴリズムを用いることができる。また、アルゴリズムＩｓｏｇ$_{L\sim,\kappa}$（Ｅ$_0$）として、図２１に示す非特許文献４，５に記載されたＩｓｏｇ$_{L\sim,\kappa}^{clg}$アルゴリズムを用いることができる。

[0157] （ステップＳ５３：同種要素生成処理）

マスター鍵生成部１４は、ステップＳ５２で生成された楕円曲線Ｅ$_t$及びトラップドアξ$_t$を用いて、φ$_t$：＝φ$_{\xi t}$と、Ｇ$_t$：＝φ$_t$（Ｇ$_0$）及びＧ＾$_t$：＝φ$_t$（Ｇ＾$_0$）と、ｇ$_t$：＝φ$_t$（ｇ$_0$）及びｇ＾$_t$：＝φ$_t$（ｇ＾$_0$）と、ｈ$_t$∈Ｇ$_t$及びｈ＾$_t$∈Ｇ＾$_t$に対してｅ$_t$（ｈ$_t$，ｈ＾$_t$）：＝ｅ$_{weil,t}$（ｈ$_t$，ｈ＾$_t$）と設定する。ここで、ｅ$_{weil,t}$は、楕円曲線Ｅ$_t$におけるヴェイユペアリングである。

[0158] （ステップＳ５４：要素出力処理）

マスター鍵生成部１４は、ステップＳ５１及びステップＳ５３で生成された（Ｇ$_t$，Ｇ＾$_t$，ｇ$_t$，ｇ＾$_t$，ｅ$_t$）$_{t\in[0,d]}$，Ｇ$_T$を公開パラメータｐｋ^{IPG}とし、（φ$_t$）$_{t\in[d]}$に対する（ξ$_t$）$_{t\in[d]}$をマスター秘密鍵ｓｋ^{IPG}として出力する。

[0159] つまり、ＩＰＧ生成アルゴリズムＧｅｎ^{IPG}（１$^{\lambda}$，ｄ）は、数１４８に示す通りである。

[数148]

$\mathrm{Gen}^{\mathrm{IPG}}(1^{\lambda},d)$:

Generate a random supersingular elliptic curve $E_0/\mathbb{F}_{p_2}$

with a sufficiently large, odd prime p, generate a suitable $(\tilde{L},\kappa)$,

$(\mathbb{G}_0,\hat{\mathbb{G}}_0,\mathbb{G}_T;e_0)$: a system of asymmetric pairing groups of order r from subgroups of E_0, where e_0 is defined by $e_0(h_0,\hat{h}_0) := e_{\mathrm{weil},0}(h_0,\hat{h}_0)^{\tilde{L}\kappa}$

for any $h_0 \in \mathbb{G}_0, \hat{h}_0 \in \hat{\mathbb{G}}_0$, from the Weil pairing $e_{\mathrm{weil},0}$ on E_0

$g_0 \xleftarrow{\mathrm{U}} \mathbb{G}_0$, $\hat{g}_0 \xleftarrow{\mathrm{U}} \hat{\mathbb{G}}_0$,

for $t \in [d]$, $(E_t,\xi_t) \xleftarrow{\mathrm{R}} \mathrm{Isog}_{\tilde{L},\kappa}(E_0)$,

$\phi_t := \phi_{\xi_t}$, $\mathbb{G}_t := \phi_t(\mathbb{G}_0)$, $\hat{\mathbb{G}}_t := \phi_t(\hat{\mathbb{G}}_0)$, $\mathrm{g}_t := \phi_t(g_0)$, $\hat{\mathrm{g}}_t := \phi_t(\hat{\mathrm{g}}_0)$,

$e_t(h_t,\hat{h}_t) := e_{\mathrm{weil},t}(h_t,\hat{h}_t)$ for any $h_t \in \mathbb{G}_t, \hat{h}_t \in \hat{\mathbb{G}}_t$,

where $e_{\mathrm{weil},t}$ is the Weil pairing $e_{\mathrm{weil},t}$ on E_t,

return $\mathrm{pk}^{\mathrm{IPG}} := ((\mathbb{G}_t,\hat{\mathbb{G}}_t,\mathrm{g}_t,\hat{\mathrm{g}}_t,e_t)_{t\in[0,d]},\mathbb{G}_T)$,

$\mathrm{sk}^{\mathrm{IPG}} := (\xi_t)_{t\in[d]}$ for $(\phi_t)_{t\in[d]}$.

[0160] ＊＊＊実施の形態５の効果＊＊＊

以上のように、実施の形態５に係る暗号システム１では、楕円曲線を用いてＩＰＧ生成アルゴリズムＧｅｎ$^{\mathrm{IPG}}$（１$^{\lambda}$，ｄ）を実現できる。

[0161] 実施の形態６.

実施の形態１～４では、記載を単純化し、理解を容易にするために、楕円曲線を用いた詳細な記載を省略した。実施の形態６では、楕円曲線を用いた具体的な構成について説明する。実施の形態６では、実施の形態１で説明したＩＢＥ方式と、実施の形態２で説明したＡＢＥ方式とについて説明する。

実施の形態３で説明したＡＢＥ方式と、実施の形態４で説明したＨＩＢＥ方式とについても、同様の方法により、楕円曲線を用いた具体的な構成とすることが可能である。

[0162] ＊＊＊動作の説明＊＊＊

実施の形態１で説明したＩＢＥ方式について説明する。

Ｓｅｔｕｐアルゴリズムは、数１４９のようになる。

[数149]

Setup(1^{λ}):

Generate a random supersingular elliptic curve $E_0/\mathbb{F}_{p_2}$

with a sufficiently large, odd prime p, generate a suitable $(\tilde{L},\kappa)$,

$(\mathbb{G}_0,\hat{\mathbb{G}}_0,\mathbb{G}_T;e_0)$: a system of asymmetric pairing groups of order r from subgroups of E_0, where e_0 is defined by $e_0(h_0,\hat{h}_0) := e_{\mathrm{weil},0}(h_0,\hat{h}_0)^{\tilde{L}\kappa}$ for any $h_0 \in \mathbb{G}_0, \hat{h}_0 \in \hat{\mathbb{G}}_0$, from the Weil pairing $e_{\mathrm{weil},0}$ on E_0

$(E_1,\xi_1) \xleftarrow{\mathrm{R}} \mathrm{Isog}_{\tilde{L},\kappa}(E_0)$,

$\phi_1 := \phi_{\xi_1}$, $\mathbb{G}_1 := \phi_1(\mathbb{G}_0)$, $\hat{\mathbb{G}}_1 := \phi_1(\hat{\mathbb{G}}_0)$,

$e_1(h_1,\hat{h}_1) := e_{\mathrm{weil},1}(h_1,\hat{h}_1)$ for any $h_1 \in \mathbb{G}_1, \hat{h}_1 \in \hat{\mathbb{G}}_1$,

where $e_{\mathrm{weil},1}$ is the Weil pairing $e_{\mathrm{weil},1}$ on E_1,

$\hat{g}_0 \xleftarrow{\mathrm{U}} \hat{\mathbb{G}}_0$, $\hat{g}_1 := \phi_1(\hat{g}_0)$,

generate a random hash $H : \mathbb{F}_q \to \mathbb{G}_0$ with the identity space $\mathbb{F}_q$,

return pk $:= ((\mathbb{G}_t,\hat{\mathbb{G}}_t,\hat{g}_t,e_t)_{t=0,1},\mathbb{G}_T,H)$, sk $:= \xi_1$ for ϕ_1.

[0163] ＫｅｙＧｅｎアルゴリズムは、数１５０のようになる。

[数150]

KeyGen(pk, sk, ID):

$h_0 := H(\mathrm{ID}) \in \mathbb{G}_0$, $h_1 := \phi_1(h_0)$,

return $\mathrm{sk}_{\mathrm{ID}} := (\mathrm{ID}, h_1)$.

[0164] Ｅｎｃアルゴリズムは、数１５１のようになる。

[数151]

$$\begin{aligned}&\mathrm{Enc}(\mathrm{pk}, m, \mathrm{ID}'):\\&h_0 := H(\mathrm{ID}'),\ \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\mathrm{X}},\\&c := \zeta \cdot \hat{g}_1,\ z := e_0(h_0, \hat{g}_0)^{\zeta \cdot \tilde{L}^{\kappa}},\ c_T := z \cdot m,\\&\text{return } \mathrm{ct}_{\mathrm{ID}'} := (\mathrm{ID}',\ c,\ c_T).\end{aligned}$$

[0165] Ｄｅｃアルゴリズムは、数１５２のようになる。

[数152]

$$\begin{aligned}&\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathrm{ID}}, \mathrm{ct}_{\mathrm{ID}'}):\\&\text{if } (\mathrm{ID} = \mathrm{ID}'),\\&\quad z' := e_1(h_1, c),\ m' := c_T \cdot (z')^{-1},\\&\quad \text{return } m'.\\&\text{otherwise, return } \perp.\end{aligned}$$

[0166] 数１５３に示すように、暗号文$\mathrm{ct}_{\mathrm{ID}'}$を復号鍵$\mathrm{sk}_{\mathrm{ID}}$で復号可能である。ここで、ｄｅｇ（$\phi_1$）＝$L^{\sim\kappa}$である。

[数153]

$$\begin{aligned}z' &:= e_1(h_1, c)\\&= e_{\mathrm{weil},1}(h_1, c)\\&= e_{\mathrm{weil},1}(\phi_1(h_0), \zeta \cdot \hat{g}_1)\\&= e_{\mathrm{weil},1}(\phi_1(h_0), \phi_1(\hat{g}_0))^{\zeta}\\&= e_{\mathrm{weil},0}(h_0, \hat{g}_0)^{\tilde{L}^{\kappa}\zeta}\\&= e_0(h_0, \hat{g}_0)^{\zeta}\\&= z\end{aligned}$$

[0167] 実施の形態２で説明したＡＢＥ方式について説明する。

Ｓｅｔｕｐアルゴリズムは、数１５４のようになる。

[数154]

Setup(1^{λ}):

Generate a random supersingular elliptic curve $E_0/\mathbb{F}_{p_2}$

with a sufficiently large, odd prime p, generate a suitable $(\tilde{L},\kappa)$,

$(\mathbb{G}_0,\hat{\mathbb{G}}_0,\mathbb{G}_T;e_0)$: a system of asymmetric pairing groups of order r from subgroups of E_0, where e_0 is defined by $e_0(h_0,\hat{h}_0) := e_{\mathrm{weil},0}(h_0,\hat{h}_0)^{\tilde{L}\kappa}$

for any $h_0 \in \mathbb{G}_0, \hat{h}_0 \in \hat{\mathbb{G}}_0$, from the Weil pairing $e_{\mathrm{weil},0}$ on E_0

$g_0 \xleftarrow{\mathrm{U}} \mathbb{G}_0$, $\hat{g}_0 \xleftarrow{\mathrm{U}} \hat{\mathbb{G}}_0$,

for $t \in [d]$, $(E_t,\xi_t) \xleftarrow{\mathrm{R}} \mathrm{Isog}_{\tilde{L},\kappa}(E_0)$,

$\phi_t := \phi_{\xi_t}$, $\mathbb{G}_t := \phi_t(\mathbb{G}_0)$, $\hat{\mathbb{G}}_t := \phi_t(\hat{\mathbb{G}}_0)$, $g_t := \phi_t(g_0)$, $\hat{g}_t := \phi_t(\hat{g}_0)$,

$e_t(h_t,\hat{h}_t) := e_{\mathrm{weil},t}(h_t,\hat{h}_t)$ for any $h_t \in \mathbb{G}_t, \hat{h}_t \in \hat{\mathbb{G}}_t$,

where $e_{\mathrm{weil},t}$ is the Weil pairing $e_{\mathrm{weil},t}$ on E_t,

generate a random hash $H : \mathbb{F}_q \to \mathbb{G}_0$ with the identity space $\mathbb{F}_q$,

return $\mathrm{pk} := ((\mathbb{G}_t,\hat{\mathbb{G}}_t,\hat{g}_t,e_t)_{t\in[0,d]},\mathbb{G}_T,H)$, $\mathrm{sk} := (\phi_t)_{t\in[d]}$.

[0168] ＫｅｙＧｅｎアルゴリズムは、数１５５のようになる。

[数155]

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

$h_0 := H(\mathrm{tag}) \in \mathbb{G}_0$,

choose random $\vec{u}$ such that $\vec{1}\cdot\vec{u} = 1$,

for $i \in [L]$, $s_i := M_i \cdot \vec{u}$, $t := \rho(i)$, $k_i := s_i \cdot \phi_t(h_0)$,

return $\mathrm{sk}_{\mathrm{tag},\mathbb{S}} := (\mathrm{tag}, \mathbb{S}, \{k_i\}_{i\in[L]})$.

[0169] Ｅｎｃアルゴリズムは、数１５６のようになる。

[数156]

$$\begin{aligned}&\mathrm{Enc}(\mathrm{pk}, m, \mathrm{tag}', \Gamma):\\ &h_0 := H(\mathrm{tag}') \in \mathbb{G}_0,\ \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q,\\ &\text{for } t \in \Gamma,\ c_t := \zeta \cdot \hat{g}_t,\ z := e_0(h_0, \hat{g}_0)^{\zeta},\ c_T := z \cdot m,\\ &\text{return } \mathrm{ct}_{\mathrm{tag}',\Gamma} := (\mathrm{tag}', \Gamma, \{c_t\}_{t\in\Gamma}, c_T).\end{aligned}$$

[0170] Ｄｅｃアルゴリズムは、数１５７のようになる。

[数157]

$$\begin{aligned}&\mathrm{Dec}(\mathrm{pk}, \mathrm{sk}_{\mathrm{tag},\mathbb{S}}, \mathrm{ct}_{\mathrm{tag}',\Gamma}):\\ &\text{if } (\mathrm{tag} = \mathrm{tag}') \text{ and } \mathbb{S} \text{ accepts } \Gamma,\\ &\quad\text{then compute}\\ &\quad\{\sigma_i\}_{\rho(i)\in\Gamma} \text{ such that } \vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i\\ &\quad\text{where } M_i \text{ is the } i\text{-th row of } M,\\ &z' = \prod_{t:=\rho(i)\in\Gamma} e_t(k_i, c_t)^{\sigma_i},\ m' := c_T \cdot (z')^{-1},\\ &\quad\text{return } m'.\\ &\text{otherwise, return } \perp.\end{aligned}$$

[0171] 数１５８に示すように、暗号文ｃｔ$_{\mathrm{ID}'}$を復号鍵ｓｋ$_{\mathrm{ID}}$で復号可能である。

[数158]

$$
\begin{aligned}
z' &= \prod_{t:=\rho(i)\in\Gamma} e_t(k_i, c_t)^{\sigma_i} \\
&= \prod_{t:=\rho(i)\in\Gamma} e_{\mathrm{weil},t}(k_i, c_t)^{\sigma_i} \\
&= \prod_{t:=\rho(i)\in\Gamma} e_{\mathrm{weil},t}(s_i \cdot \phi_t(h_0), \zeta \cdot \hat{g}_t)^{\sigma_i} \\
&= \prod_{t:=\rho(i)\in\Gamma} e_{\mathrm{weil},t}(\phi_t(h_0), \phi_t(\hat{g}_0))^{\zeta\sigma_i s_i} \\
&= \prod_{t:=\rho(i)\in\Gamma} e_{\mathrm{weil},0}(h_0, \hat{g}_0)^{\tilde{L}_K \zeta\sigma_i s_i} \\
&= e_{\mathrm{weil},0}(h_0, \hat{g}_0)^{\tilde{L}_K \zeta} \\
&= e_0(h_0, \hat{g}_0)^{\zeta} \\
&= z
\end{aligned}
$$

[0172] ＊＊＊実施の形態６の効果＊＊＊

以上のように、実施の形態６に係る暗号システム１では、楕円曲線を用いて具体的にＩＢＥ方式及びＡＢＥ方式を構成することができる。

[0173] 実施の形態７．

実施の形態１～６では、同種写像とペアリング演算とを用いて、ＩＰＧを構成した。し

かし、同種写像に代えて、トラップドア準同型写像（以下、ＴＨ）を用いてＩＰＧを構成してもよい。

[0174] 以下の３つの条件を満たす場合、素数位数ｑの２つのランダムに選択された巡回群G_0，G_1についての写像$\phi := \phi_\xi : G_0 \to G_1$がＴＨである。

（条件１：準同型写像）

写像φが自明でない準同型写像であること。自明でないとは、例えば、加法群に対して非ゼロであることである。

（条件２：ＴＨ－ＤＨ（ＴＨ－Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）の難治性仮定）

ランダムに選択された写像φと群G_0から一様に選択されたg_0，gについて、（g_0，φ（g_0），g）が与えられた場合に、どんな確率的多項式時間マシンBも無視し得る確率でしかφ（g）を計算しないこと。

（条件３：多項式サイズのトラップドア）

φ：＝ϕ_ξについての多項式サイズのトラップドアξが与えられると、どんなg∈G_0に対してもφ（g）を計算する確率的多項式時間マシンBが存在すること。

[0175] 楕円曲線を用いたTHの例として以下の３つがある。以下の３つの例において、群の肩に“～”が付されている場合、その群はペアリング群である。

（例１：累乗法）

G_0：＝G_1：＝G~は、楕円曲線巡回群である。φ：＝ϕ_ξは、群Gにおける累乗法、つまり曲線上のスカラー乗法である。つまり、ϕ_ξ：g→g^ξである。ここで、ξはスカラーである。

（例２：ペアリング）

G_0：＝G~，G_1：＝$G~_T$は、ペアリング群である。φ：＝ϕ_ξは、G~上のペアリング演算である。つまり、ϕ_ξ：g→e（g，ξ）である。ここで、ξは、対称ペアリングの場合の群G、又は、非対称ペアリングの場合の群G^の要素である。

（例３：同種写像）

G_0：＝$G~_0$，G_1：＝$G~_1$は、それぞれ２つの曲線E，E’から得られる２つの異なる楕円曲線巡回群である。φ：＝ϕ_ξは、群$G~_0$から群$G~_1$への同種写像である。つまり、ϕ_ξ：E→E’：＝E／Cである。ここで、ξ：＝Cは、曲線Eの巡回部分群である。

符号の説明

[0176] １　暗号システム、１０　鍵生成装置、１１　プロセッサ、１２　記憶装置、１３　入出力インタフェース、１４　マスター鍵生成部、１５　復号鍵生成部、１６　鍵出力部、２０　暗号化装置、２１　プロセッサ、２２　記憶装置、２３　入出力インタフェース、２４　入力受付部、２５　暗号文生

成部、２６　暗号文出力部、３０　復号装置、３１　プロセッサ、３２　記憶装置、３３　入出力インタフェース、３４　入力受付部、３５　復号部、３６　メッセージ出力部。

請求の範囲

[請求項1] 同種写像とペアリング演算とによって対応付けられた複数の群を用いた暗号システムにおける暗号化装置であり、

前記複数の群のうちのある群の暗号要素を含む暗号文を生成する暗号文生成部を備える暗号化装置。

[請求項2] 前記暗号システムは、群G_0と、前記群G_0と同種写像ϕ_tによって対応付けられた群G_tと、前記群G_0及び群$G\hat{}_0$とペアリング演算e_0によって対応付けられるとともに、前記群G_t及び群$G\hat{}_t$とペアリング演算e_tによって対応付けられた群G_Tとを用いる

請求項１に記載の暗号化装置。

[請求項3] 前記暗号文は、前記群G_0の要素と前記群$G\hat{}_0$の要素とについて前記ペアリング演算e_0を行うことにより生成された前記群G_Tの要素ｚを含む暗号要素c_Tと、前記群$G\hat{}_t$の要素である暗号要素ｃとを含む請求項２に記載の暗号化装置。

[請求項4] 前記暗号システムは、ｔ＝１の整数ｔについての前記群G_t及び前記群$G\hat{}_t$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素c_Tとして、数１に示す要素ｃ，c_Tを含む請求項３に記載の暗号化装置。

[数1]

$$c := \hat{g}_1^{\zeta},$$
$$c_T := z \cdot m$$

ここで、

$\hat{g}_1 \in \hat{\mathbb{G}}_1$,

ζは値,

$z := e_0(h_0, \hat{g}_0)^{\zeta}$,

mはメッセージ,

$h_0 \in \mathbb{G}_0$,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[請求項5] 前記暗号システムは、２以上の整数ｄに関してｔ＝０，．．．．，ｄの整数ｔについての群G_t及び群$\hat{G}_t$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素c_Tとして、数２に示す要素c_t，c_Tを含む請求項３に記載の暗号化装置。

[数2]

$$c_t := \hat{g}_t^{\zeta} \text{ for } t \in \Gamma,$$
$$c_T := z \cdot m$$

ここで、

$\hat{g}_t \in \hat{\mathbb{G}}_t$,

ζは値,

$z := e_0(h_0, \hat{g}_0)^{\zeta}$,

mはメッセージ,

$h_0 \in \mathbb{G}_0$,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[請求項6] 前記暗号システムは、１以上の整数ｄ及び１以上の整数ｎに関してｔ＝０，．．．，ｄの整数ｔとｊ＝０，．．．，ｎの整数ｎとι＝０，１の整数ιとについての群$G_{t,j,\iota}$及び群$\hat{G}_{t,j,\iota}$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素c_Tとして、数３に示す要素$c_{t,j}$，c_Tを含む請求項３に記載の暗号化装置。

[数3]

$$c_{t,j} := \hat{g}_{t,j,x_{t,j}}^{\zeta} \text{ for } (t, x_t := (x_{t,j}) \in \{0,1\}^n) \in \Gamma,$$

$$c_T := z \cdot m$$

ここで、

$\hat{g}_{t,j,\iota} \in \hat{\mathbb{G}}_{t,j,\iota}$,

ζ は値,

$z := e_0(h_0, \hat{g}_0)^{\zeta}$,

m はメッセージ,

$h_0 \in \mathbb{G}_0$,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[請求項7] 前記暗号システムは、ｔ＝１の整数ｔについての前記群Ｇ$_t$及び前記群Ｇ＾$_t$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素ｃ$_T$として、数９に示す要素ｃ＾$_0$，ｃ$_i$，ｃ$_T$を含む請求項３に記載の暗号化装置。

[数4]

$$\hat{c}_0 := \hat{g}_1^{\zeta},$$

$$c_i := h_i^{\zeta}, h_i := \mathrm{H}_1(\mathrm{ID}_1,...,\mathrm{ID}_i) \text{ for } i \in [2, j],$$

$$c_T := z \cdot m$$

ここで、

$\hat{g}_1 \in \hat{\mathbb{G}}_1$,

ζ は値,

$\mathrm{ID}_1,...,\mathrm{ID}_j$ は値,

$z := e_0(h_1, \hat{g}_0)^{\zeta}$,

m はメッセージ,

$h_1 := \mathrm{H}_0(\mathrm{ID}_1)$,

$\mathrm{H}_0, \mathrm{H}_1$ は $\mathrm{ID}_1,...,\mathrm{ID}_j$ の空間の要素を $\mathbb{G}_0$ の要素に変換する関数,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[請求項8] 同種写像とペアリング演算とによって対応付けられた複数の群を用いた暗号システムにおける復号装置であり、

前記複数の群のうちのある群の暗号要素を含む暗号文を、前記複数の群のうちの前記ある群とは異なる群の鍵要素を含む復号鍵を用いて復号する復号部

を備える復号装置。

[請求項9] 前記暗号システムは、群G_0と、前記群G_0と同種写像ϕ_tによって対応付けられた群G_tと、前記群G_0及び群$G\hat{}_0$とペアリング演算e_0によって対応付けられるとともに、前記群G_t及び群$G\hat{}_t$とペアリング演算e_tによって対応付られた群G_Tとを用いる

請求項８に記載の復号装置。

[請求項10] 前記暗号文は、前記群G_0の要素と前記群$G\hat{}_0$の要素とについて前記ペアリング演算e_0を行うことにより生成された前記群G_Tの要素ｚを含む暗号要素c_Tと、前記群$G\hat{}_t$の要素である暗号要素ｃとを含み、

前記復号鍵は、前記群G_tの鍵要素ｋを含み、

前記復号部は、前記鍵要素ｋと前記暗号要素ｃとについて前記ペアリング演算e_tを行い要素ｚ’を計算し、計算された前記要素ｚ’と前記暗号要素c_Tとを用いて前記暗号文を復号する

請求項９に記載の復号装置。

[請求項11] 前記暗号システムは、ｔ＝１の整数ｔについての前記群G_t及び前記群$G\hat{}_t$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素c_Tとして、数５に示す要素ｃ，c_T

を含み、

前記復号鍵は、前記鍵要素ｋとして、数６に示す要素h_1を含み、

前記復号部は、前記要素h_1と前記要素ｃとについて、ペアリング演算e_1を行い、前記暗号文を復号する

請求項１０に記載の復号装置。

[数5]

$$c := \hat{g}_1^{\zeta},$$
$$c_T := z \cdot m$$

ここで、

$\hat{g}_1 \in \hat{\mathbb{G}}_1$,

ζ は値,

$z := e_0(h_0, \hat{g}_0)^{\zeta}$,

m はメッセージ,

$h_0 \in \mathbb{G}_0$,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[数6]

$$h_1 := \phi_1(h_0)$$

[請求項12] 前記暗号システムは、２以上の整数ｄに関してｔ＝０，．．．．，ｄの整数ｔについての群Ｇ$_t$及び群Ｇ＾$_t$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素ｃ$_T$として、数７に示す要素ｃ$_t$，ｃ$_T$を含み、

前記復号鍵は、前記鍵要素ｋとして、数８に示す要素ｋ$_i$を含み、

前記復号部は、前記要素ｃ$_t$と前記要素ｋ$_i$について、数９に示すペアリング演算を行い、前記暗号文を復号する

請求項１０に記載の復号装置。

[数7]

$$c_t := \hat{g}_t^{\zeta} \text{ for } t \in \Gamma,$$
$$c_T := z \cdot m$$

ここで、

$\hat{g}_t \in \hat{\mathbb{G}}_t$,

ζは値,

$z := e_0(h_0, \hat{g}_0)^{\zeta}$,

mはメッセージ,

$h_0 \in \mathbb{G}_0$,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[数8]

$$k_i := \phi_t(h_0)^{s_i}$$

ここで、

スパンプログラム$S := (M, \rho)$,

$s_i := M_i \cdot \vec{u}$,

M_iはMのｉ行目,

$\vec{u} \cdot \vec{1} = 1$,

$t = \rho(i)$

[数9]

$$z' := \prod_{t=\rho(i)\in\Gamma} e_t(k_i, c_t)^{\sigma_i}$$

ここで、

$$\vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i$$

[請求項13] 前記暗号システムは、１以上の整数ｄ及び１以上の整数ｎに関して

ｔ＝０，．．．，ｄ

の整数ｔとｊ＝０，．．．，ｎの整数ｎとι＝０，１の整数ιとにつ

いての群$G_{t,j,\iota}$及び群$\hat{G}_{t,j,\iota}$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素c_Tとして、数１０に示す要素$c_{t,j}$，c_Tを含み、

前記復号鍵は、前記鍵要素ｋとして、数１１に示す要素$k_{i,j}$を含み、

前記復号部は、前記要素$c_{t,j}$と前記要素$k_{i,j}$について、数１２に示すペアリング演算を行い、前記暗号文を復号する

請求項１０に記載の復号装置。

[数10]

$$c_{t,j} := \hat{g}_{t,j,x_{t,j}}^{\zeta} \text{ for } (t, x_t := (x_{t,j}) \in \{0,1\}^n) \in \Gamma,$$

$$c_T := z \cdot m$$

ここで、

$\hat{g}_{t,j,\iota} \in \hat{\mathbb{G}}_{t,j,\iota}$,

ζは値,

$z := e_0(h_0, \hat{g}_0)^{\zeta}$,

mはメッセージ,

$h_0 \in \mathbb{G}_0$,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[数11]

$$k_{i,j} := \phi_{t,j,v_{i,j}}(h_0)^{\tau_{i,j}} \text{ for } i \in [L]$$

ここで、

スパンプログラム $S := (M, \rho)$,

L は M の行数,

$s_i := M_i \cdot \vec{u}$,

M_i は M の i 行目,

$\vec{u} \cdot \vec{1} = 1$,

$\vec{\tau}_i := (\tau_{i,j})$ such that $s_i = \sum_{j=1}^{n} \tau_{i,j}$,

$\rho(i) = (t, v_i := (v_{i,j}) \in \{0,1\}^n)$

[数12]

$$z' := \prod_{\rho(i)=(t,(v_{i,j}))\in\Gamma} \left(\prod_{j=1}^{n} e_{t,j,v_{i,j}}(k_{i,j}, c_{t,j}) \right)^{\sigma_i}$$

ここで、

$\vec{1} = \sum_{\rho(i)\in\Gamma} \sigma_i M_i$

[請求項14] 前記暗号システムは、ｔ＝１の整数ｔについての前記群Ｇ$_t$及び前記群Ｇ＾$_t$を用い、

前記暗号文は、前記暗号要素ｃ及び前記暗号要素ｃ$_T$として、数１３に示す要素ｃ＾$_0$，ｃ$_i$，ｃ$_T$を含み、

前記復号鍵は、前記鍵要素ｋとして数１４に示す要素ｄ＾$_i$，ｄ$_j$を含み、

前記復号部は、前記要素ｃ＾$_0$，ｃ$_i$と前記要素ｄ＾$_i$，ｄ$_j$について、数１５に示すペアリング演算を行い、前記暗号文を復号する

請求項１０に記載の復号装置。

[数13]

$$\hat{c}_0 := \hat{g}_1^{\zeta},$$

$$c_i := h_i^{\zeta},\ h_i := \mathrm{H}_1(\mathrm{ID}_1,...,\mathrm{ID}_i) \text{ for } i \in [2, j],$$

$$c_T := z \cdot m$$

ここで、

$\hat{g}_1 \in \hat{\mathbb{G}}_1$,

ζ は値,

$\mathrm{ID}_1,...,\mathrm{ID}_j$ は値,

$z := e_0(h_1, \hat{g}_0)^{\zeta}$,

m はメッセージ,

$h_1 := \mathrm{H}_0(\mathrm{ID}_1)$,

$\mathrm{H}_0, \mathrm{H}_1$ は $\mathrm{ID}_1,...,\mathrm{ID}_j$ の空間の要素を $\mathbb{G}_0$ の要素に変換する関数,

$\hat{g}_0 \in \hat{\mathbb{G}}_0$

[数14]

$$\hat{d}_i := \hat{g}_1^{r_i} \in \hat{\mathbb{G}}_1 \text{ for } i \in [j-1],$$

$$d_j := \phi_1(h_1) \cdot \prod_{i=2}^{j} h_i^{r_{i-1}}$$

ここで、

r_i は値,

$h_1 := \mathrm{H}_0(\mathrm{ID}_1)$,

$h_i := \mathrm{H}_1(\mathrm{ID}_1,...,\mathrm{ID}_i) \text{ for } i \in [2, j]$,

[数15]

$$z' := \frac{e_1(d_i, \hat{c}_0)}{\prod_{i=2}^{j} e_1(c_i, \hat{d}_{i-1})}$$

[請求項15] 同種写像とペアリング演算とによって対応付けられた複数の群を用いた暗号システムであり、

前記複数の群のうちのある群の暗号要素を含む暗号文を生成する暗号化装置と、

前記複数の群のうちの前記ある群とは異なる群の鍵要素を含む復号鍵を用いて、前記暗号化装置によって生成された暗号文を復号する復号装置と

を備える暗号システム。

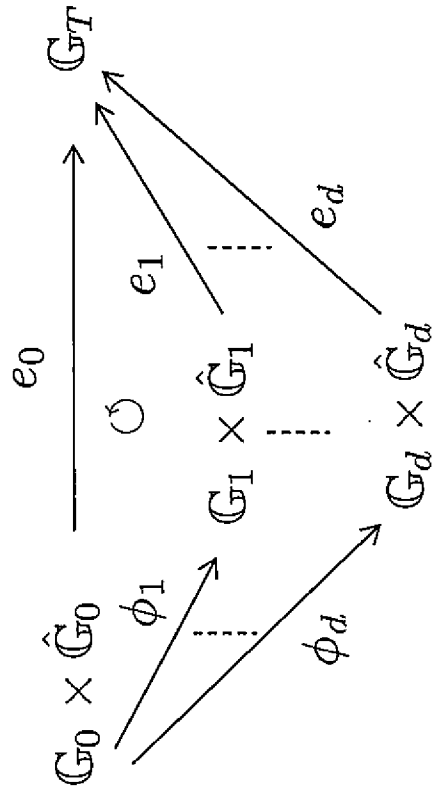
[請求項16] 群G_0と、前記群G_0と準同型写像ϕ_tによって対応付けられた群G_tと、前記群G_0及び群$G\hat{}_0$とペアリング演算e_0によって対応付られるとともに、前記群G_t及び群$G\hat{}_t$とペアリング演算e_tによって対応付られた群G_Tとを用いた暗号システムであり、

前記群G_0の要素と、前記群$G\hat{}_0$の要素とについて前記ペアリング演算e_0を行うことにより生成された前記群G_Tの要素zを含む前記暗号要素c_Tと、前記群$G\hat{}_t$の要素である暗号要素cとを含む暗号文を生成する暗号化装置と、

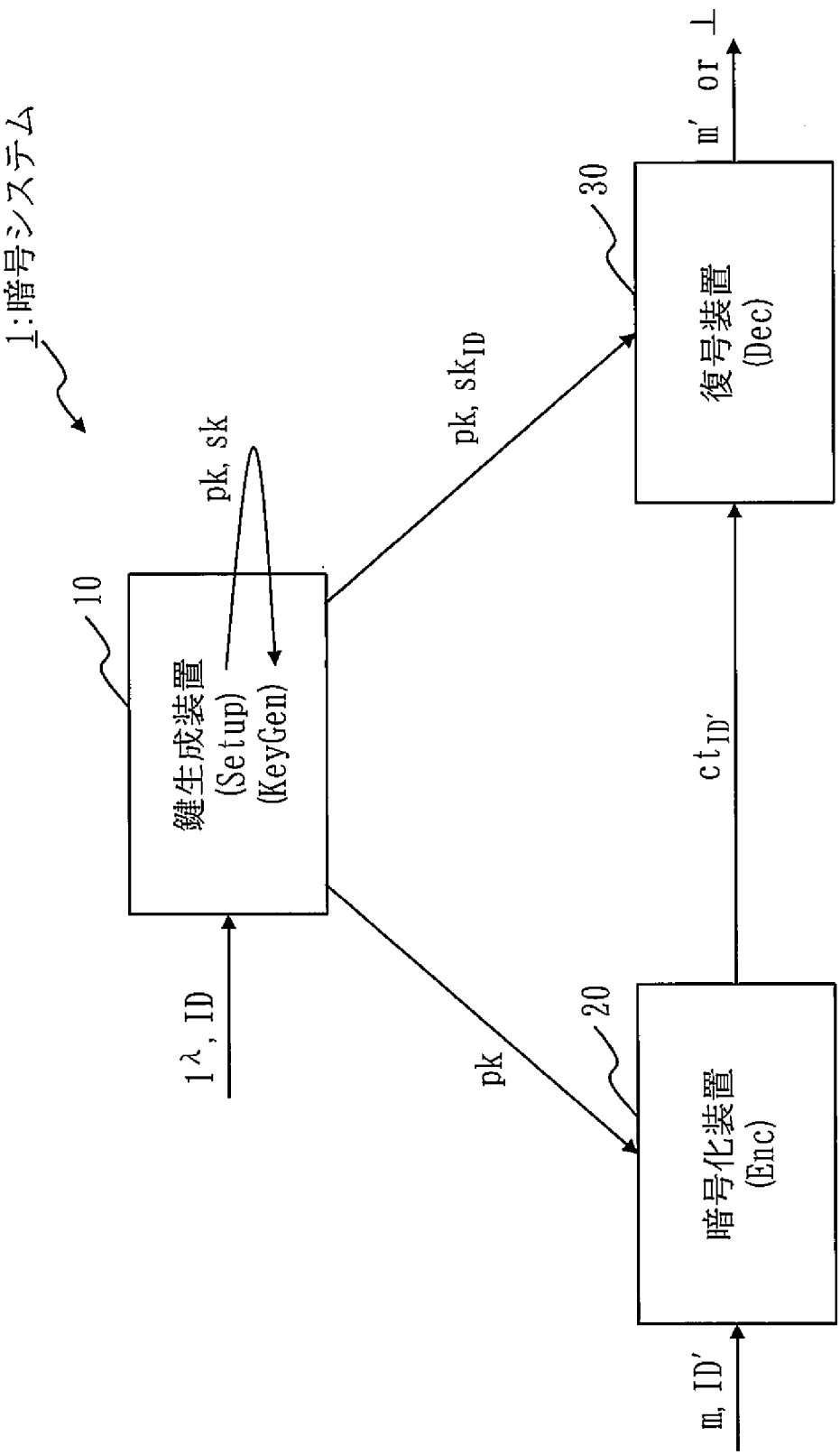
前記群G_tの鍵要素kを含む復号鍵を用いて、前記鍵要素kと前記暗号要素cとについて前記ペアリング演算e_tを行い要素z'を計算し、計算された前記要素z'と前記暗号要素c_Tとを用いて前記暗号文を復号する復号装置と

を備える暗号システム。

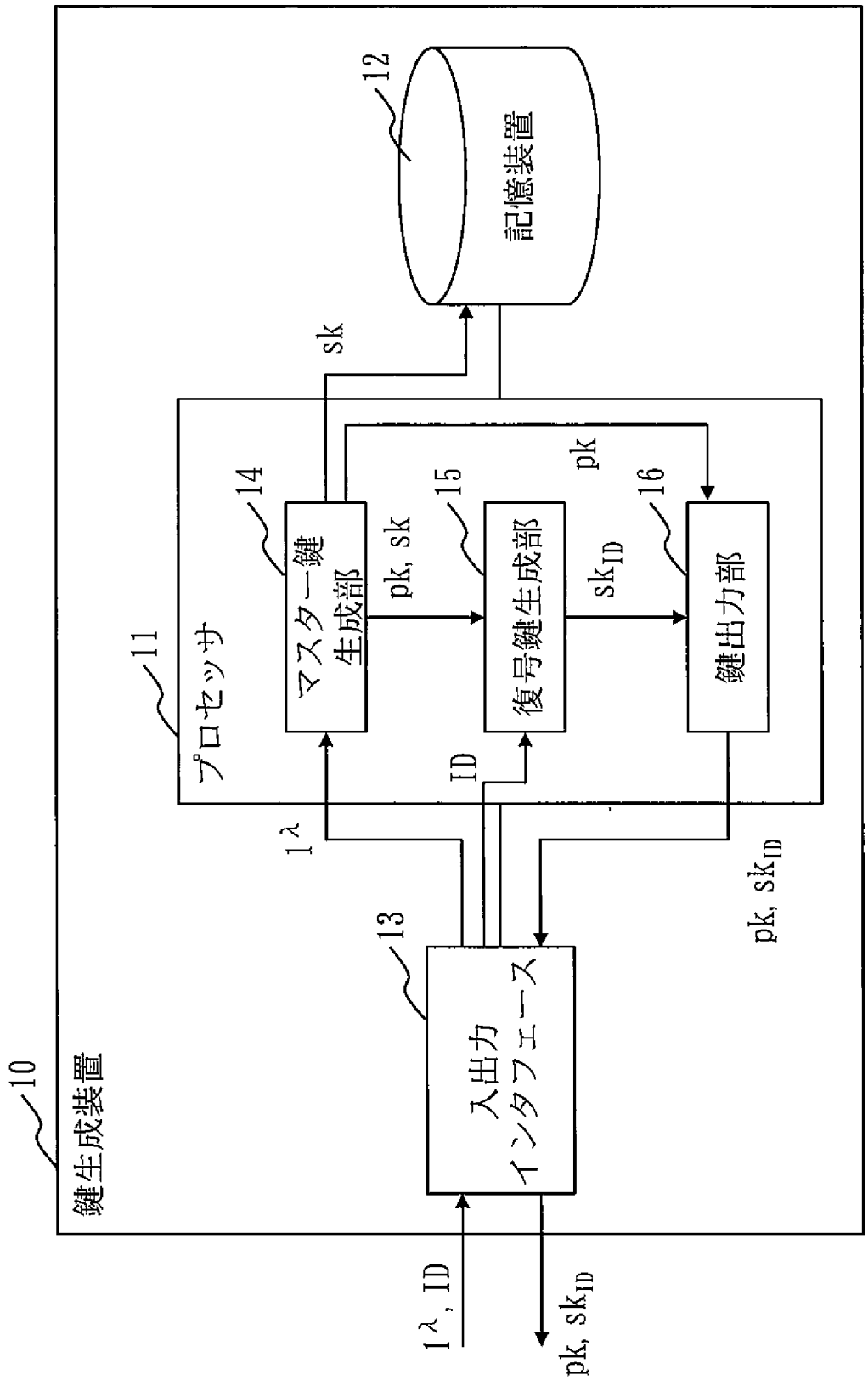
[図1]


$\mathbb{G}_T$
e_0
e_1
e_d
$\mathbb{G}_0 \times \hat{\mathbb{G}}_0$
$\mathbb{G}_1 \times \hat{\mathbb{G}}_1$
$\mathbb{G}_d \times \hat{\mathbb{G}}_d$
ϕ_1
ϕ_d

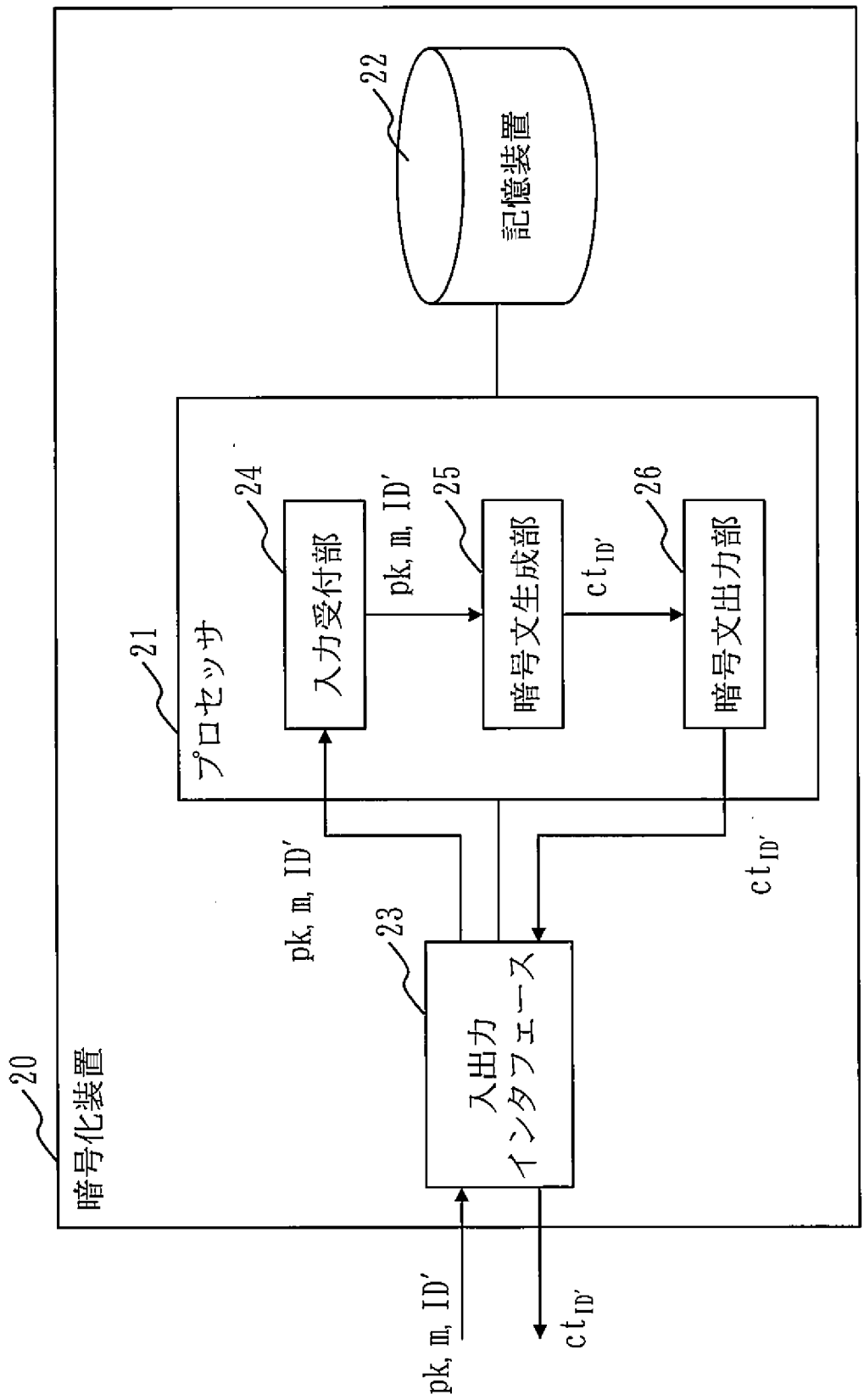
[図2]


1:暗号システム
鍵生成装置
(Setup)
(KeyGen)
10
pk, sk
pk, sk_ID
復号装置
(Dec)
30
m′ or ⊥
1^λ, ID
pk
暗号化装置
(Enc)
20
ct_ID′
m, ID′

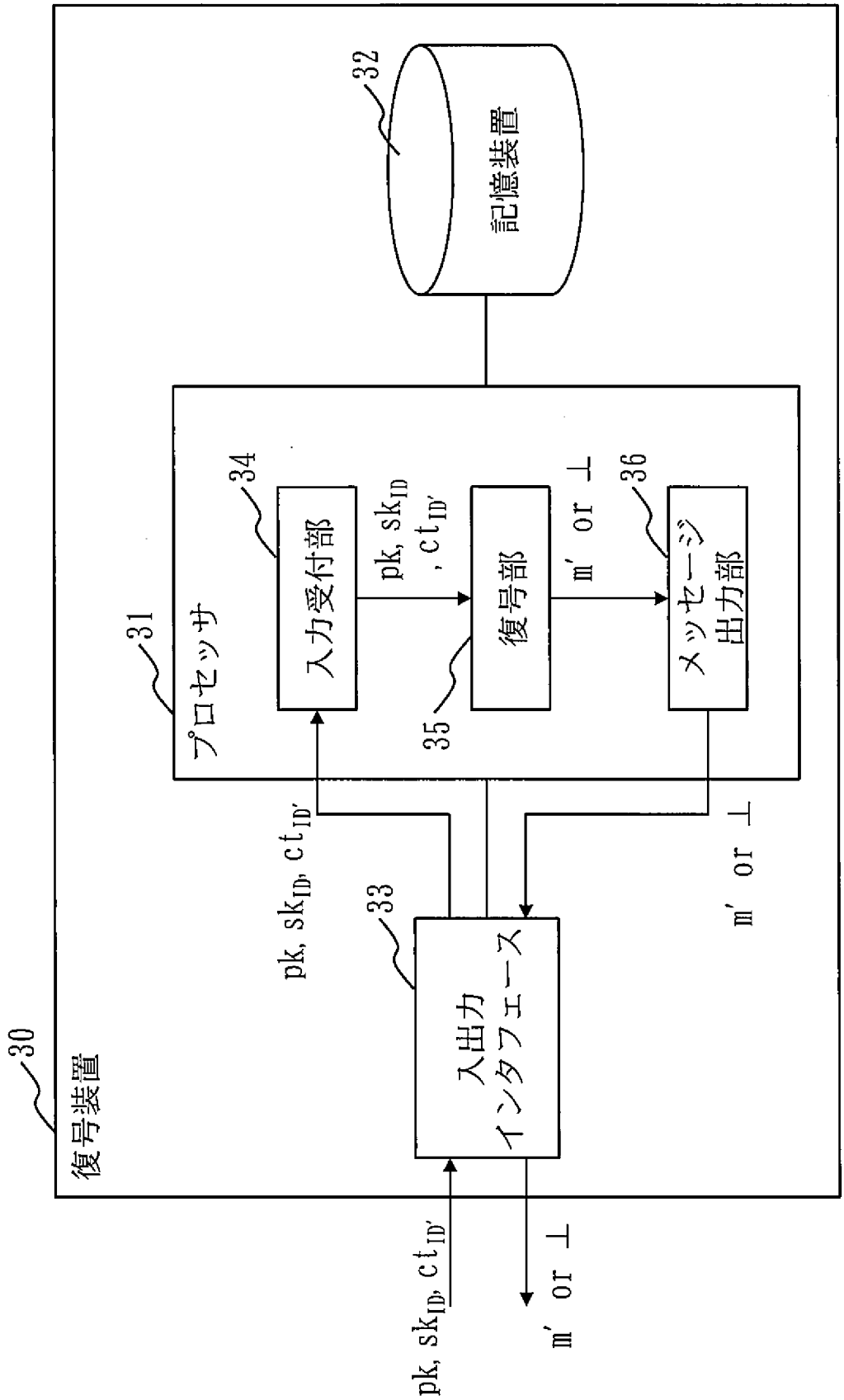
[図3]


10
鍵生成装置
11
プロセッサ
12
記憶装置
13
入出力
インタフェース
14
マスター鍵
生成部
15
復号鍵生成部
16
鍵出力部
sk
pk
pk, sk
sk_{ID}
ID
1^{λ}
1^{λ}, ID
pk, sk_{ID}
pk, sk_{ID}

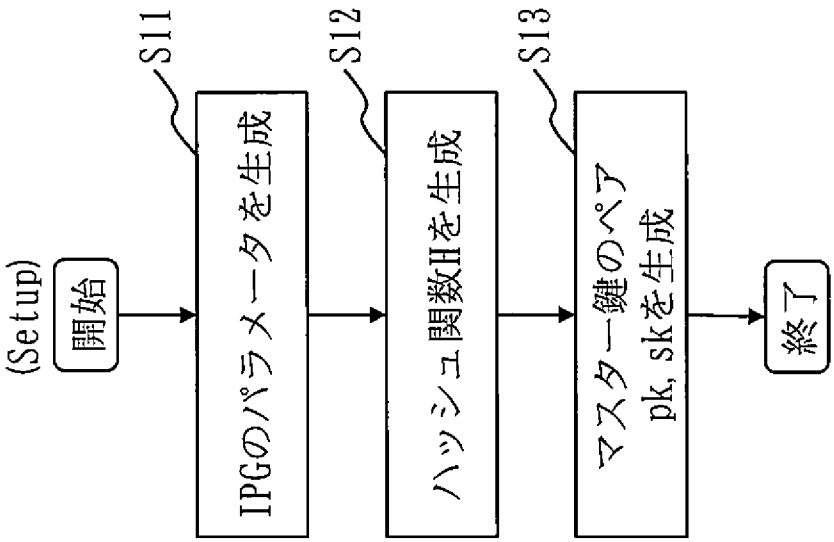
[図4]


20
暗号化装置
21
プロセッサ
22
記憶装置
23
入出力
インタフェース
24
入力受付部
25
暗号文生成部
26
暗号文出力部
pk, m, ID′
pk, m, ID′
ct_ID′
pk, m, ID′
ct_ID′
ct_ID′

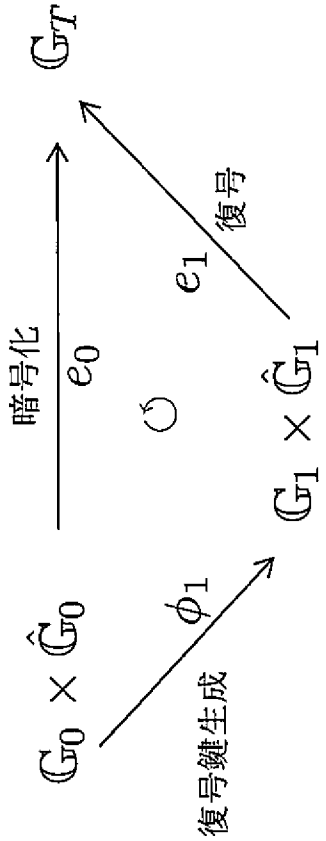
[図5]


30
復号装置
31
プロセッサ
32
記憶装置
33
入出力
インタフェース
34
入力受付部
35
復号部
36
メッセージ
出力部
pk, sk_ID, ct_ID'
pk, sk_ID
, ct_ID'
m' or ⊥
pk, sk_ID, ct_ID'
m' or ⊥
m' or ⊥

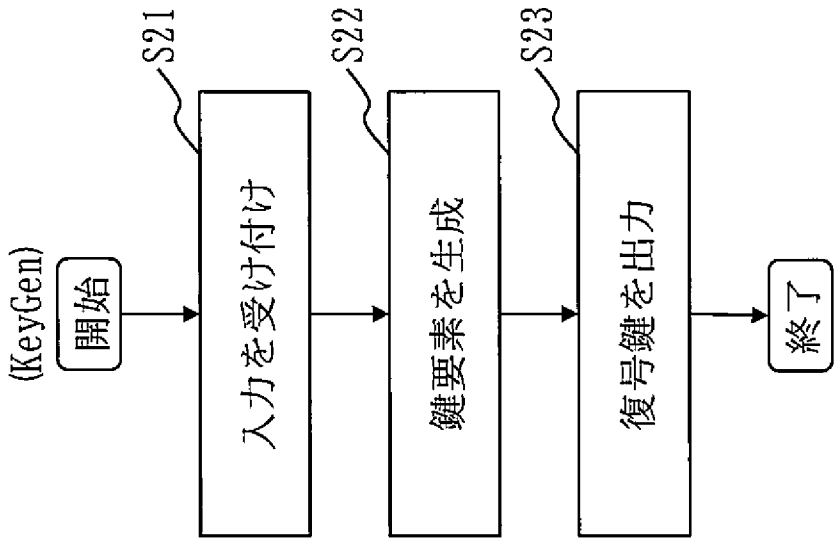
[図6]


(Setup)
開始
S11
IPGのパラメータを生成
S12
ハッシュ関数Hを生成
S13
マスター鍵のペア
pk, skを生成
終了

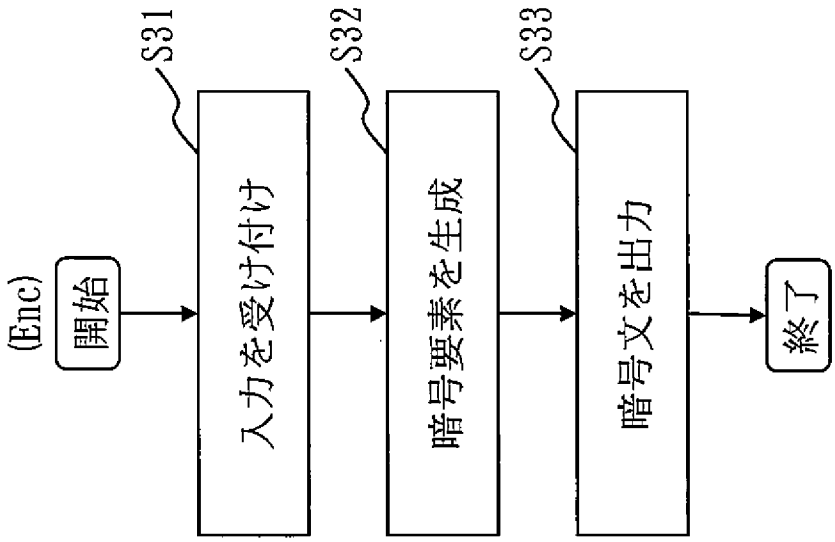
[図7]


$\mathbb{G}_T$
暗号化
e_0
e_1
復号
$\mathbb{G}_0 \times \hat{\mathbb{G}}_0$
ϕ_1
$\mathbb{G}_1 \times \hat{\mathbb{G}}_1$
復号鍵生成

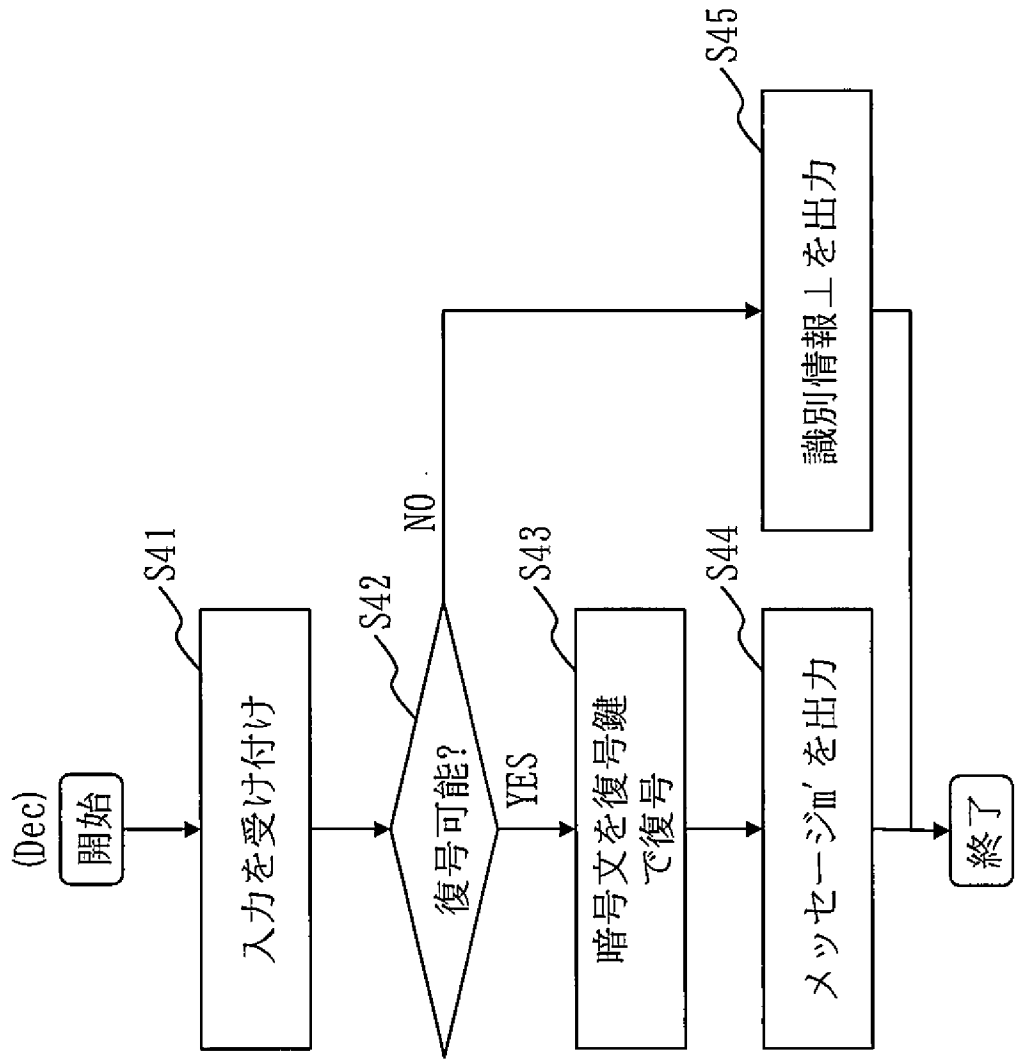
[図8]



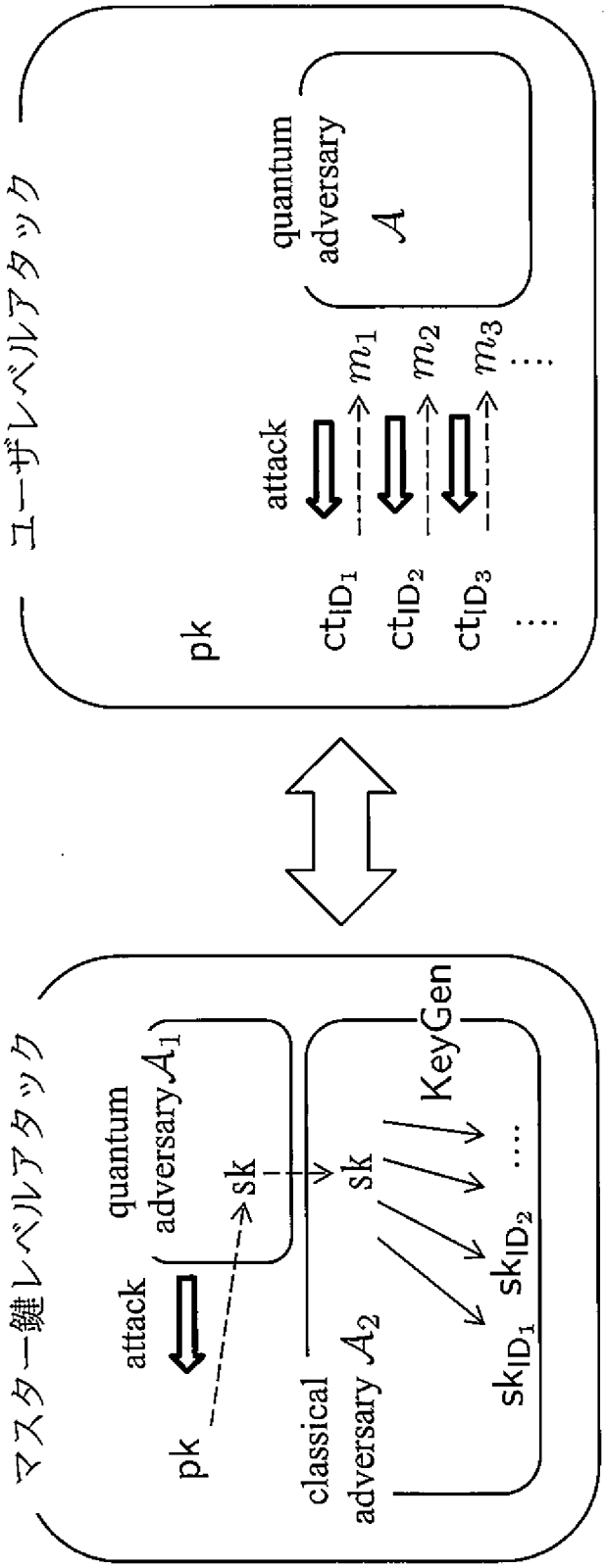
[図9]



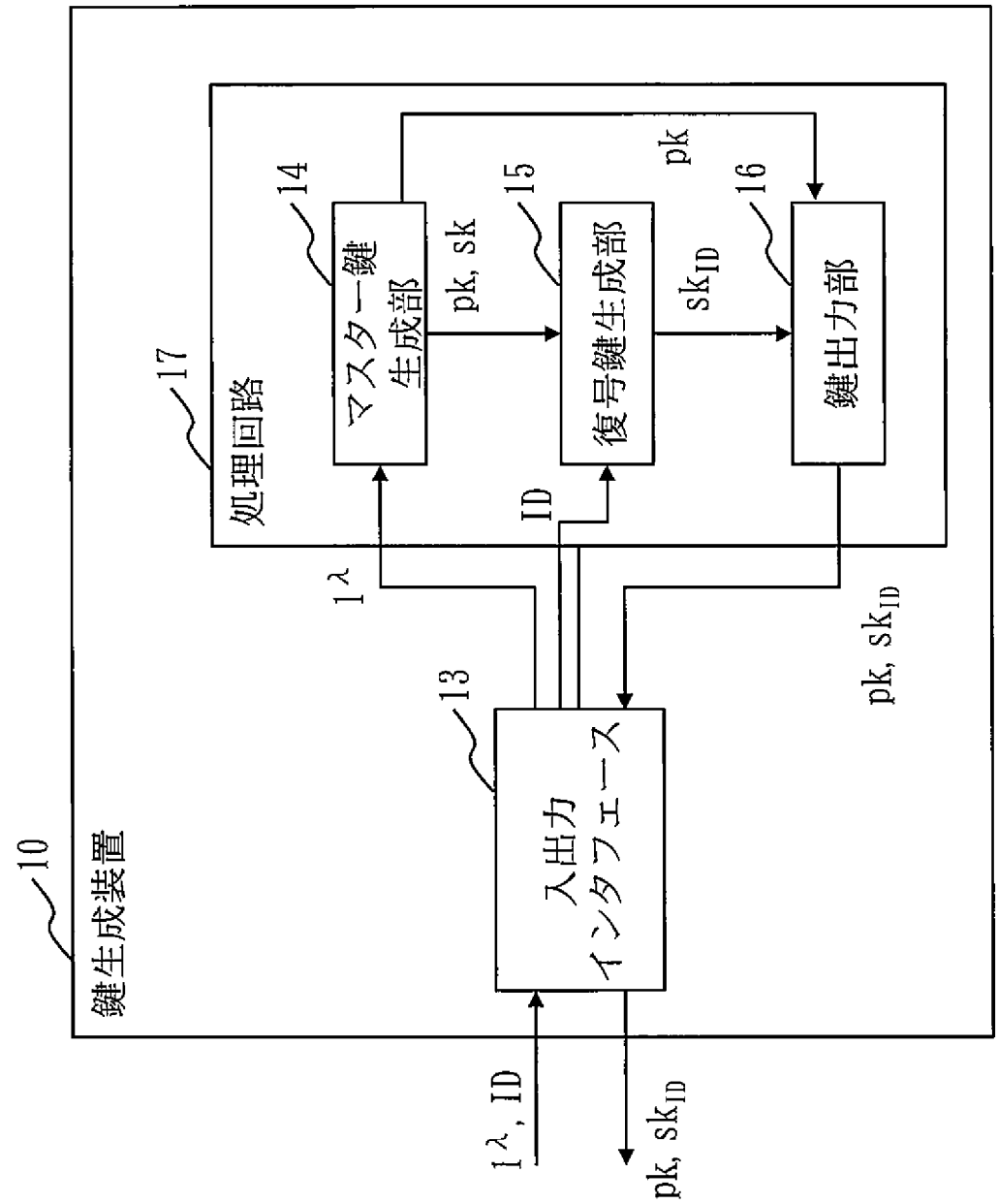
[図10]


(Dec)
開始
S41
入力を受け付け
S42
復号可能?
NO
YES
S43
暗号文を復号鍵で復号
S44
メッセージm'を出力
S45
識別情報⊥を出力
終了

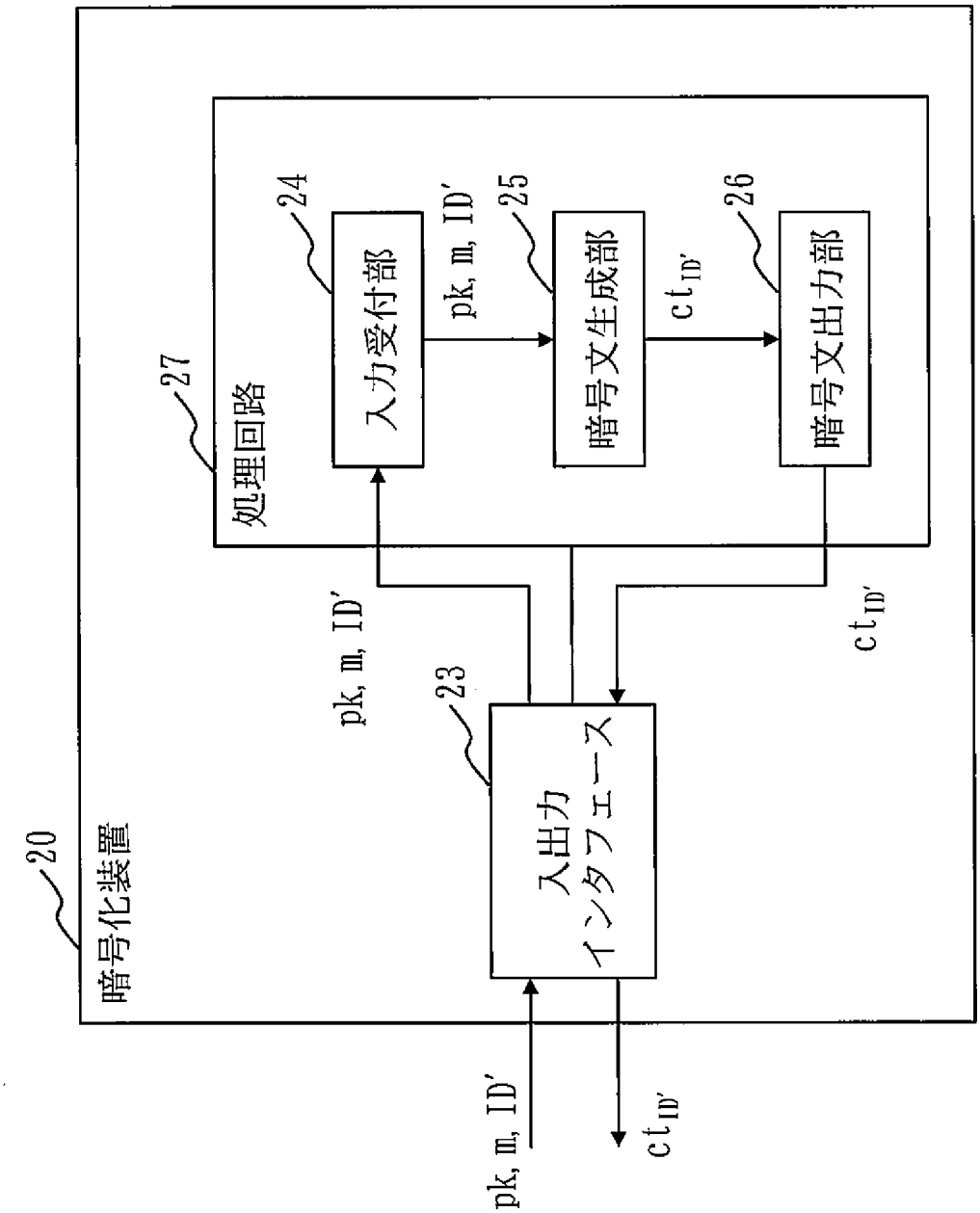
[図11]


ユーザレベルアタック
pk
attack
quantum adversary $\mathcal{A}$
ct_{ID_1} ct_{ID_2} ct_{ID_3} ....
m_1 m_2 m_3 ....
マスター鍵レベルアタック
pk
attack
quantum adversary $\mathcal{A}_1$
sk
classical adversary $\mathcal{A}_2$
KeyGen
sk
sk_{ID_1} sk_{ID_2} ....

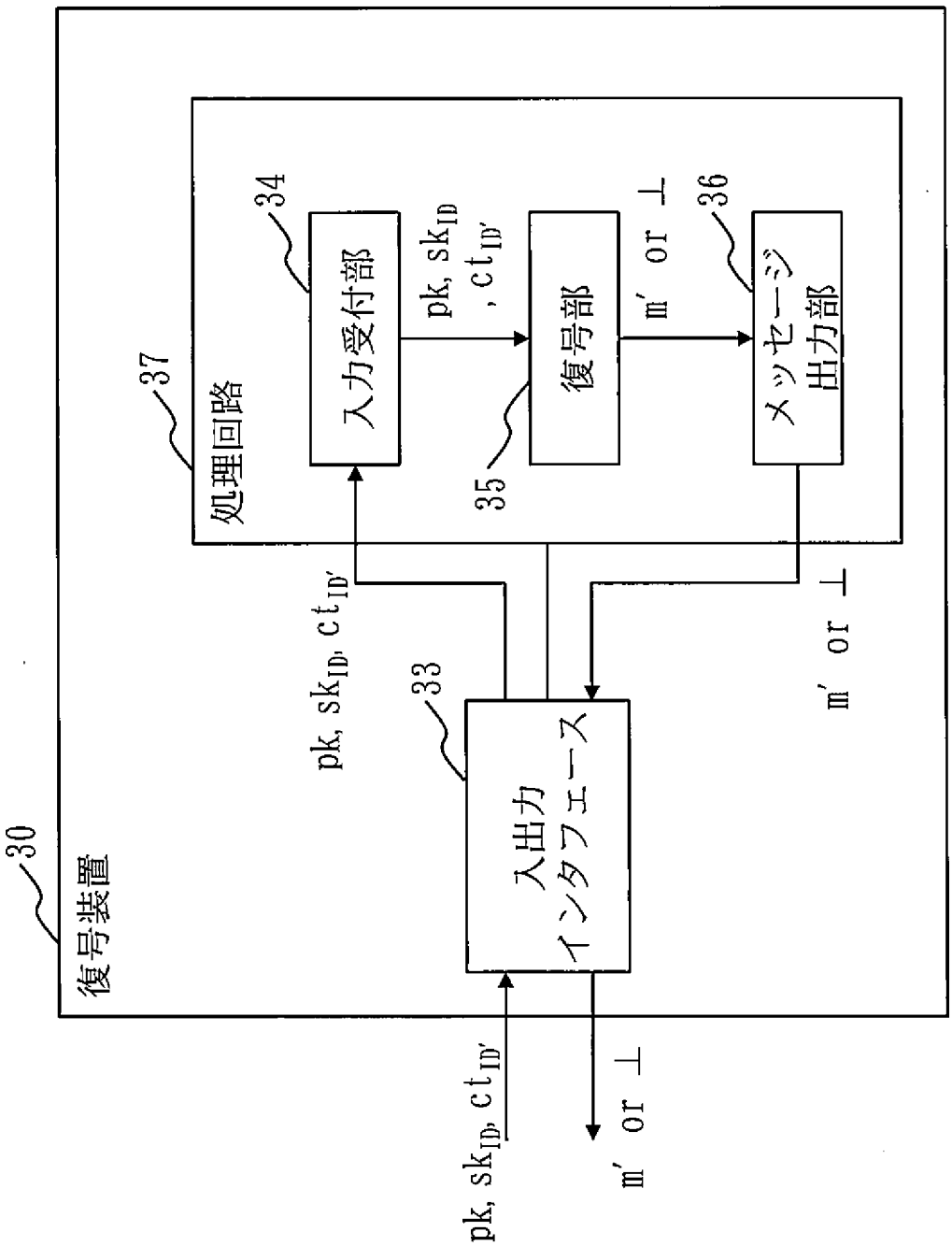
[図12]


10
鍵生成装置
17
処理回路
14
マスター鍵
生成部
15
復号鍵生成部
16
鍵出力部
13
入出力
インタフェース
pk, sk
pk
ID
1λ
pk, sk_ID
1λ, ID
pk, sk_ID

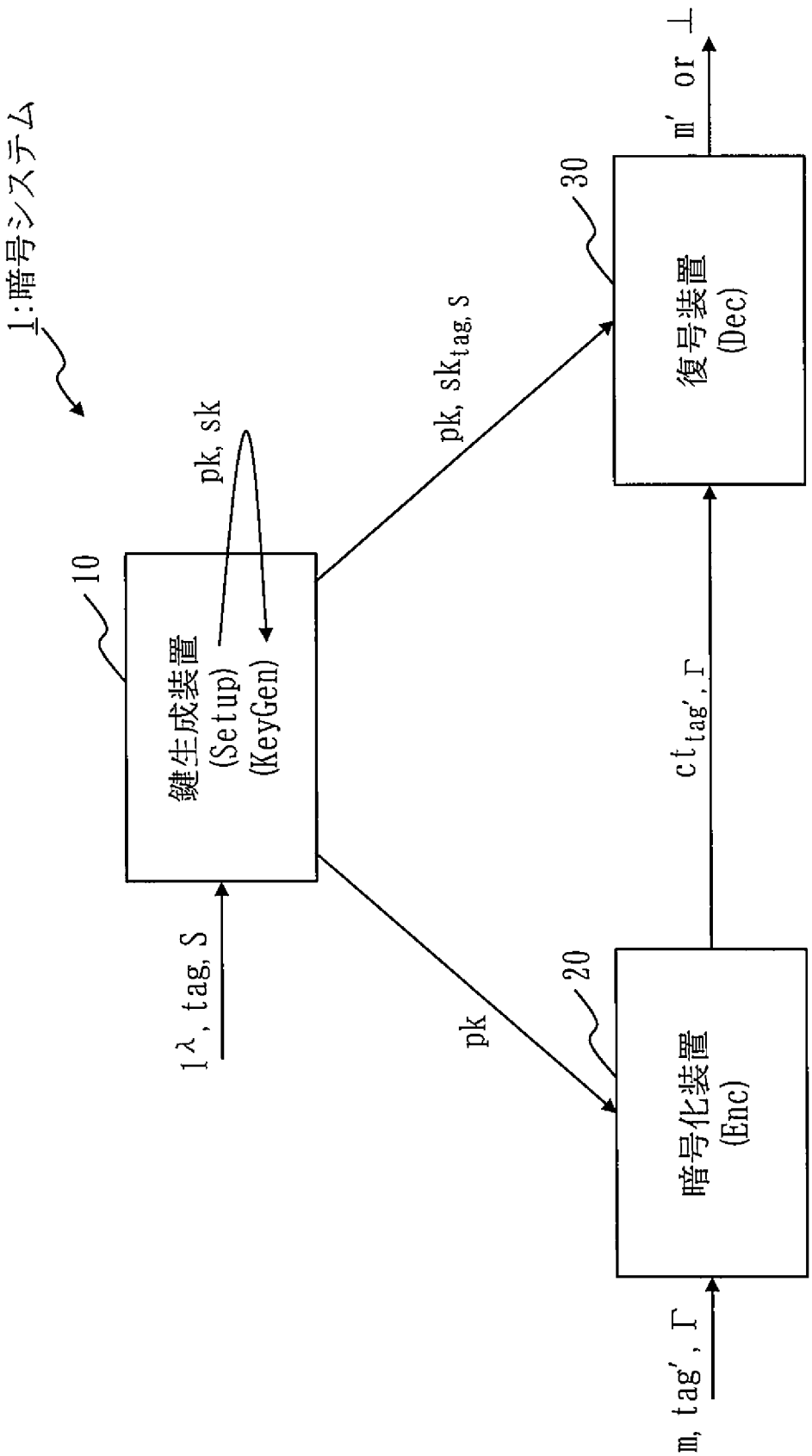
[図13]


20
暗号化装置
27
処理回路
24
入力受付部
25
暗号文生成部
26
暗号文出力部
23
入出力
インタフェース
pk, m, ID'
pk, m, ID'
ct_ID'
pk, m, ID'
ct_ID'

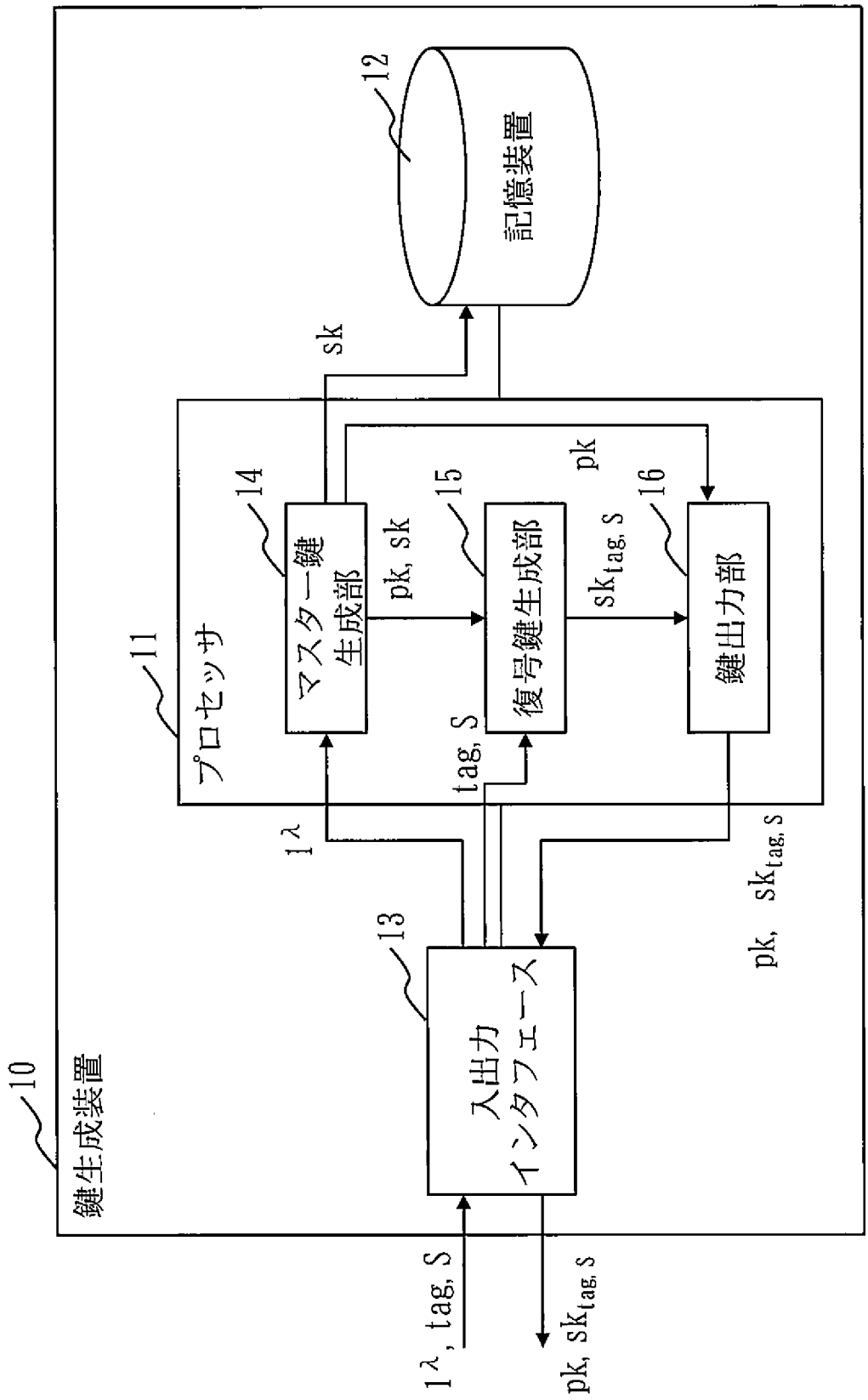
[図14]


30
復号装置
37
処理回路
34
入力受付部
pk, sk_{ID} , $ct_{ID'}$
35
復号部
m′ or ⊥
36
メッセージ出力部
pk, sk_{ID}, $ct_{ID'}$
33
入出力インタフェース
m′ or ⊥
pk, sk_{ID}, $ct_{ID'}$
m′ or ⊥

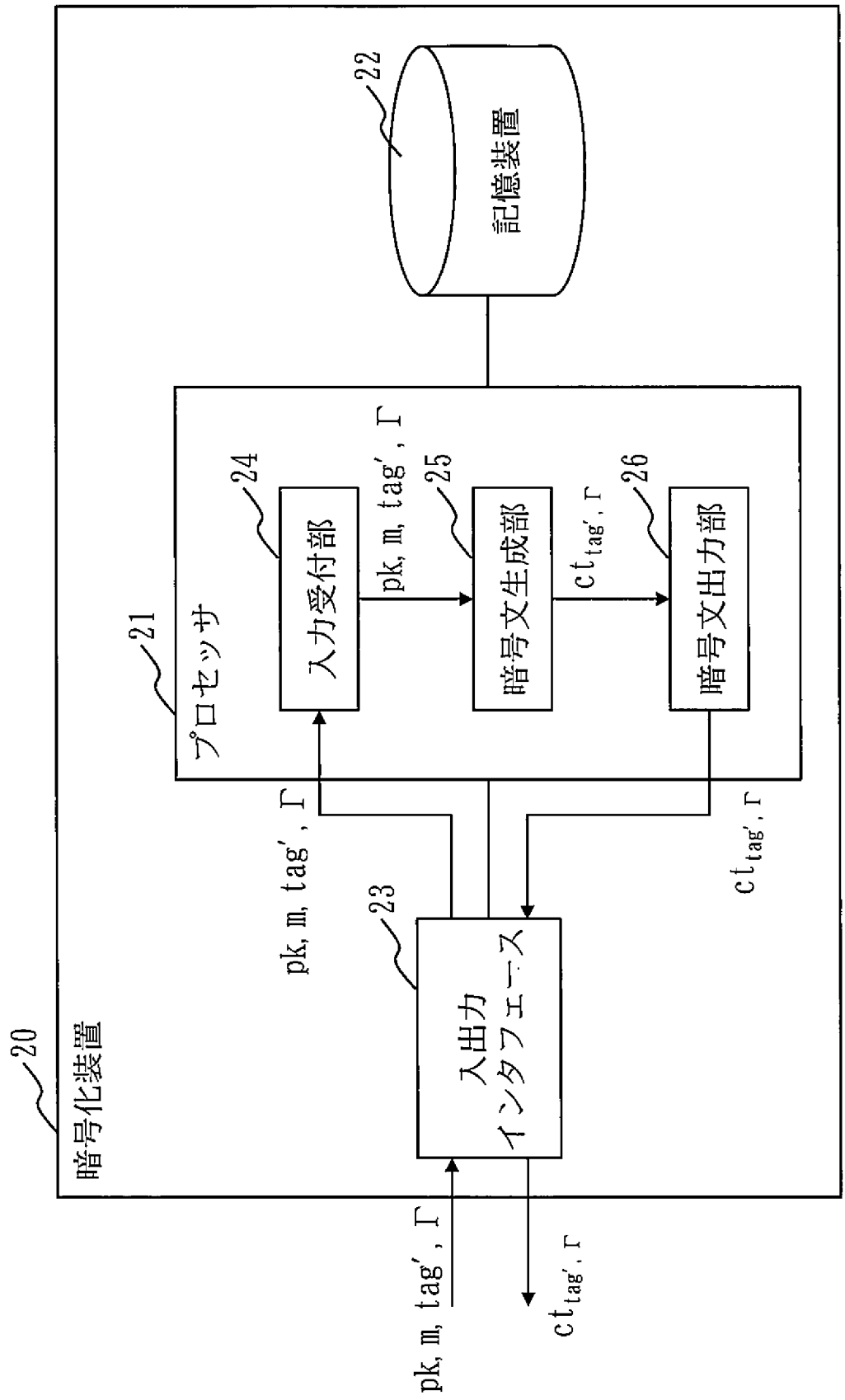
[図15]


1:暗号システム
10
鍵生成装置
(Setup)
(KeyGen)
pk, sk
pk, sk$_{tag, S}$
30
復号装置
(Dec)
m′ or ⊥
1$^{\lambda}$, tag, S
pk
20
暗号化装置
(Enc)
ct$_{tag′, Γ}$
m, tag′, Γ

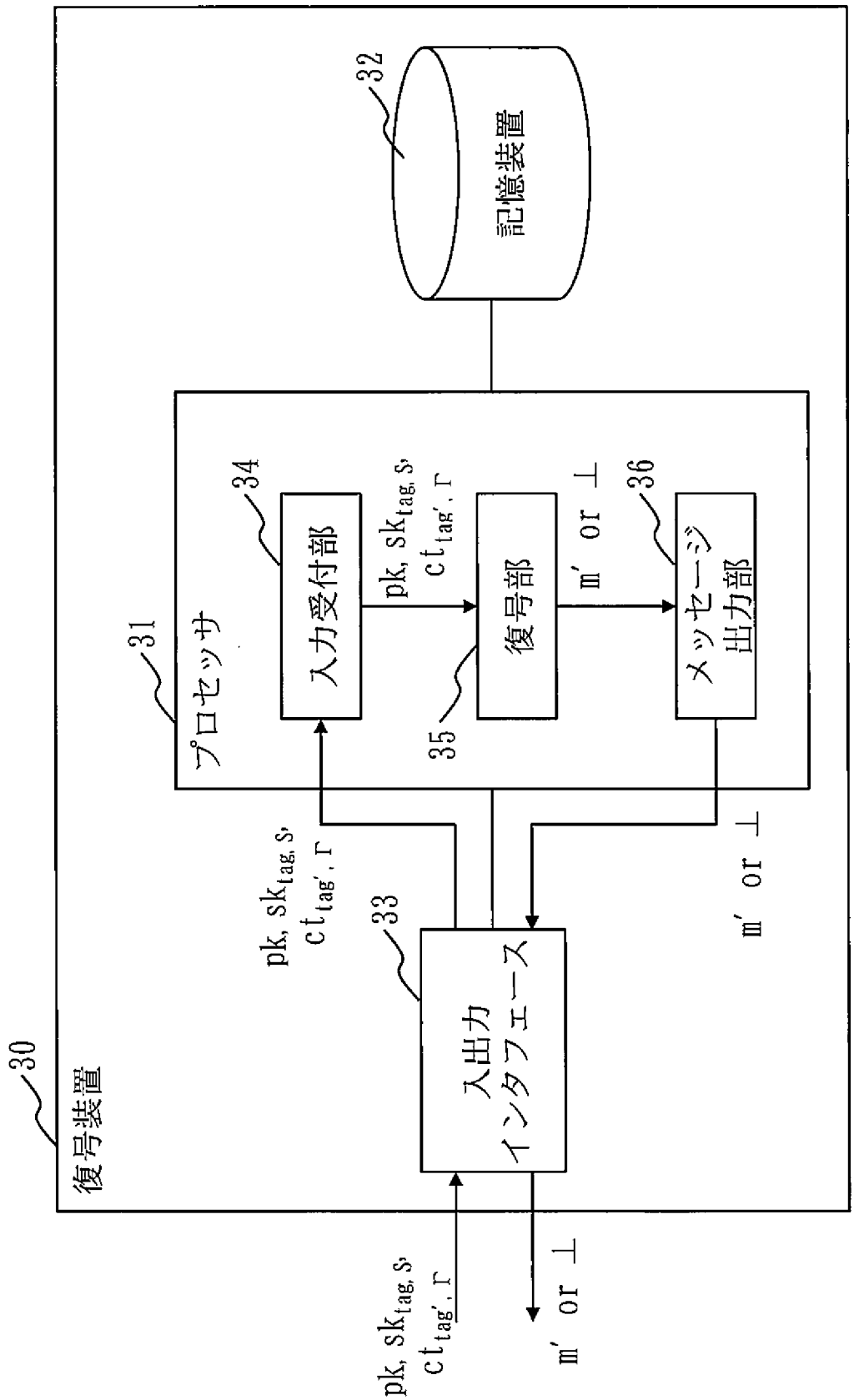
[図16]


10
鍵生成装置
11
プロセッサ
12
記憶装置
13
入出力
インタフェース
14
マスター鍵
生成部
15
復号鍵生成部
16
鍵出力部
sk
pk
pk, sk
tag, S
$sk_{tag, S}$
1^{λ}
1^{λ}, tag, S
pk, $sk_{tag, S}$

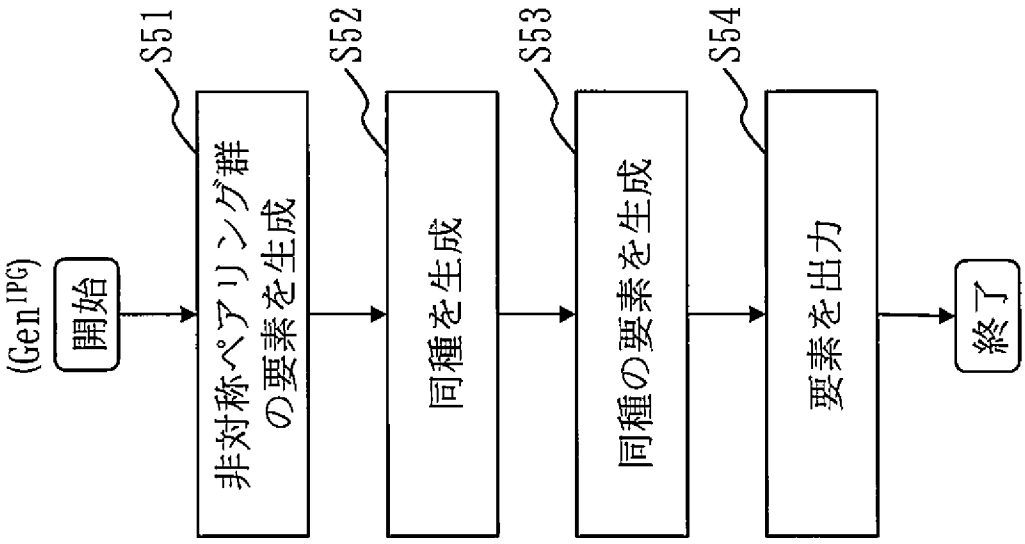
[図17]


20
暗号化装置
21
プロセッサ
22
記憶装置
23
入出力
インタフェース
24
入力受付部
25
暗号文生成部
26
暗号文出力部
pk, m, tag′, Γ
pk, m, tag′, Γ
ct_tag′, Γ
pk, m, tag′, Γ
ct_tag′, Γ
ct_tag′, Γ

[図18]


30
復号装置
31
プロセッサ
32
記憶装置
33
入出力
インタフェース
34
入力受付部
35
復号部
36
メッセージ
出力部
pk, sk$_{tag, s}$,
ct$_{tag', r}$
m′ or ⊥
pk, sk$_{tag, s}$,
ct$_{tag', r}$
m′ or ⊥
pk, sk$_{tag, s}$,
ct$_{tag', r}$
m′ or ⊥

[図19]


(Gen^IPG)
開始
S51
非対称ペアリング群の要素を生成
S52
同種を生成
S53
同種の要素を生成
S54
要素を出力
終了

[図20]

Algorithm 1 Isog^djp_$\tilde{L}$,κ :
Generate a random supersingular EC which is $\tilde{L}^{\kappa}$-isogenous to E_0

Input : An initial elliptic curve E_0.
Output : An isogenous E and a kernel generator R in $E_0[\tilde{L}^{\kappa}]$, that is,
a trapdoor ξ for computing the isogeny $\varphi := \varphi_\xi : E_0 \rightarrow E$.
1: generate a random point R in $E_0[\tilde{L}^{\kappa}]$, then set $R_0 := R$
2: for $0 \leq i < \kappa$ do
3: compute $E_{i+1} := E_i/\langle \tilde{L}^{\kappa-i-1}R_i \rangle$, $\psi_i : E_i \rightarrow E_{i+1}$, and $R_{i+1} := \psi_i(R_i)$ by Velu's formula, where $R_i \in E_i[\tilde{L}^{\kappa-i}]$, $\tilde{L}^{\kappa-i-1}R_i$ is in $E_i[\tilde{L}]$ and then ψ_i is an $\tilde{L}$-isogeny.
4: end for
5: we set the composition $\varphi := \psi_{\kappa-1} \cdots \psi_0 : E_0 \rightarrow E_\kappa = E_0/\langle R \rangle$.
return $E := E_\kappa$ (or $j(E_\kappa)$) and $\xi := R$

[図21]

Algorithm 2 Isog^clg_$\tilde{L}$,κ :
Generate a random supersingular EC which is $\tilde{L}^{\kappa}$-isogenous to E_0 when = 2

Input : An initial elliptic curve E_0.
Output : An isogenous E and all the selector bits $\omega := \{\omega_i\}_{0\leq i<\kappa}$, that is,
a trapdoor ξ for computing the isogeny $\varphi := \varphi_\xi : E_0 \rightarrow E$.

1: for $0 \leq i < \kappa$ do
2: generate a random bit $\omega_i \in \{0, 1\}$ for selecting a next kernel point R_i,
which is either of two points in $K_i := E_i[\tilde{L}] \mid \psi_{i-1}(E_{i-1}[\tilde{L}])$ if $i \neq 0$
(resp., in $K_i := \{$ some fixed two points in $E_i[\tilde{L}] \mid \{O_{Ei}\}\}$ if $i = 0$) since = 2.
3: compute $E_i/\langle R_i\rangle$ and the j-invariants $j(E_i/\langle R_i\rangle)$ by Velu's formula for two
candidates $R_i \in K_i$.
4: $j(E_i/\langle R_i\rangle)$ i.e., R_i, is determined from ω_i by a lexicographic order in F_{p2} .
5: we set $\psi_i : E_i \rightarrow E_{i+1} := E_i/\langle R_i\rangle$ for the selected R_i.
6: end for
7: we set the composition $\varphi := \psi_{\kappa-1} \ldots \psi_0 : E_0 \rightarrow E_\kappa$.
return $E := E_\kappa$ (or $j(E_\kappa)$) and all the selector bits $\xi := \omega := \{\omega_i\}_{0\leq i<\kappa}$.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/001558

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2017
Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017

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.
X Y	JP 2005-141200 A (Microsoft Corp.), 02 June 2005 (02.06.2005), paragraphs [0020] to [0059], [0132] to [0157] & US 2005/0094806 A1 paragraphs [0026] to [0042], [0085] to [0096] & EP 1528705 A1 & DE 602004020565 D & CA 2483486 A & BR 404122 A & NO 20044028 A & NZ 535698 A & IL 164071 D & KR 10-2005-0042441 A & CN 1614922 A & ZA 200407941 A & BR PI0404122 A & AT 429098 T & SG 111191 A & CO 5630049 A & HK 1085585 A & RU 2004132057 A & AU 2004218638 A & MX PA04010155 A & TW 200525979 A & CA 2483486 A1	1-6,8-13, 15-16 7,14

☒ 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
11 April 2017 (11.04.17)	18 April 2017 (18.04.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/001558

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	GENTRY, Craig and SILVERBERG, Alice, Hierarchical ID-Based Cryptography, Lecture Notes in Computer Science, 2002, Vol. 2501, pp. 248-566	7,14
A	JP 2006-311477 A (Microsoft Corp.), 09 November 2006 (09.11.2006), & US 2006/0248338 A1 & EP 1717724 A1 & CA 2517807 A & KR 10-2006-0113329 A & CN 1855815 A & BR PI0503555 A & AU 2005203526 A & RU 2005127358 A & CA 2517807 A1	1-16
P,X	KOSHIBA, Takeshi and TAKASHIMA, Katsuyuki, Pairing Cryptography Meets Isogeny: A New Framework of Isogenous Pairing Groups, Cryptology ePrint Archive [online], Report 2016/1138, Ver. 20161214:185829, 2016.12, pp. 1-36, [retrieved on 2017.04.07], Retrieved from the Internet: <URL: http://eprint.iacr.org/2016/1138/20161214:185829>	1-16

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／００１５５８

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, G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７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
X	JP 2005-141200 A (マイクロソフト　コーポレーション)	1-6, 8-13,
	2005.06.02, 段落 0020-0059, 0132-0157	15-16
Y	& US 2005/0094806 A1, 段落 0026-0042, 0085-0096	7, 14
	& EP 1528705 A1 & DE 602004020565 D & CA 2483486 A	
	& BR 404122 A & NO 20044028 A & NZ 535698 A & IL 164071 D	
	& KR 10-2005-0042441 A & CN 1614922 A & ZA 200407941 A	
	& BR PI0404122 A & AT 429098 T & SG 111191 A & CO 5630049 A	
	& HK 1085585 A & RU 2004132057 A & AU 2004218638 A	
	& MX PA04010155 A & TW 200525979 A & CA 2483486 A1	

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１１．０４．２０１７	１８．０４．２０１７

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
Y	GENTRY, Craig and SILVERBERG, Alice, Hierarchical ID-Based Cryptography, Lecture Notes in Computer Science, 2002, Vol. 2501, pp. 248-566	7, 14
A	JP 2006-311477 A (マイクロソフト　コーポレーション) 2006.11.09, & US 2006/0248338 A1 & EP 1717724 A1 & CA 2517807 A & KR 10-2006-0113329 A & CN 1855815 A & BR PI0503555 A & AU 2005203526 A & RU 2005127358 A & CA 2517807 A1	1-16
P, X	KOSHIBA, Takeshi and TAKASHIMA, Katsuyuki, Pairing Cryptography Meets Isogeny: A New Framework of Isogenous Pairing Groups, Cryptology ePrint Archive [online], Report 2016/1138, Ver. 20161214:185829, 2016.12, pp. 1-36, [retrieved on 2017.04.07], Retrieved from the Internet: <URL: http://eprint.iacr.org/2016/1138/20161214:185829>	1-16