

明 細 書

発明の名称：再暗号化鍵生成装置、再暗号化装置及びプログラム
技術分野

[0001] 本発明の実施形態は、再暗号化鍵生成装置、再暗号化装置及びプログラムに関する。

背景技術

[0002] ユーザがサーバにファイルをアップロードし、複数ユーザ間でそのファイルを共有するファイル共有システムにおいて、サーバに対してファイルデータの秘匿性を保つ方法として以下の三つの方式（１）～（３）が挙げられる。

[0003] （１）各ユーザに個別の暗号化鍵でファイルを暗号化する個別鍵方式。

[0004] （２）各ユーザに共通の暗号化鍵でファイルを暗号化する共通鍵方式。

[0005] （３）プロキシ再暗号化方式を用いてファイルを暗号化する再暗号化方式。

[0006] 上記（１）～（３）の方式において、サーバにファイルをアップロードするユーザをユーザＡとし、ユーザＡがユーザＢ、ユーザＣとファイルを共有するとする。

[0007] （１）の個別鍵方式では、ユーザ毎に異なる秘密鍵と公開鍵の組を各ユーザがそれぞれ持つ。ユーザＡは、ユーザＢの公開鍵でファイルを暗号化し、暗号化されたファイルをサーバへアップロードする。なお、ユーザＢの公開鍵は、ユーザＢに個別の暗号化鍵である。同様に、ユーザＡは、ユーザＣの公開鍵でファイルを暗号化し、暗号化されたファイルをサーバへアップロードする。ユーザＣの公開鍵は、ユーザＣに個別の暗号化鍵である。つまり、ユーザＡは、ファイルを共有する全てのユーザそれぞれに対して個別にファイルを暗号化する。

[0008] （２）の共通鍵方式では、各ユーザに共通の秘密鍵と公開鍵の組を各ユーザが共有する。ユーザＡは、（各ユーザに共通の暗号化鍵である）公開鍵で

ファイルを暗号化し、暗号化されたファイルをサーバへアップロードする。
各ユーザは、同一の秘密鍵を共有している。

[0009] (3) のプロキシ再暗号化方式では、(1) の個別鍵方式と同様に、ユーザ毎に異なる秘密鍵と公開鍵の組を各ユーザがそれぞれ持つ。しかしながら、(1) の個別鍵方式とは異なり、ユーザAは、ユーザのグループを管理するエンティティ（以下、グループ管理者と呼ぶ）の公開鍵（以下、グループ公開鍵と呼ぶ）でファイルを暗号化すれば良い。サーバは、（ユーザAがアップロードした）暗号化ファイルを、再暗号化鍵に基づいてそれぞれ再暗号化する。再暗号化により、各ユーザだけが復号できる暗号化ファイルが生成される。プロキシ再暗号化方式の詳細は後述する。

[0010] (1) の個別鍵方式では、新たにユーザDともファイルを共有したいとき、ユーザAがユーザDの公開鍵でファイルを暗号化し、暗号化されたファイルをサーバへアップロードする必要があるという不都合がある。なお、ユーザDの公開鍵は、ユーザDに個別の暗号化鍵である。従って、(1) の方法は、新規ユーザ数や共有ファイル数が多い場合に、新規ユーザ追加時の処理が煩雑となるため、ファイル共有システムに不適である。

[0011] (2) の共通鍵方式では、あるユーザに対するファイル共有の許可をある時点から取り消す（当該ユーザをファイル共有システムから排除する）際に、各ユーザに共通の秘密鍵と公開鍵を更新する機構が別途必要である不都合がある。また、(2) の共通鍵暗号方式では、各ユーザに共通の秘密鍵が万が一漏洩してしまった場合、当該漏洩した秘密鍵を入手した者には、全ての暗号化ファイルが復号可能になってしまう不都合がある。このため、(2) の共通鍵方式は、ファイル共有システムに不適である。

[0012] 一方、(3) のプロキシ再暗号化方式では、サーバが再暗号化鍵を用いて一つの暗号文を各ユーザだけが復号できる暗号文に再暗号化するため、ユーザに再暗号化鍵を知らせない構成にして、上述した不都合を解決している。このため、(3) のプロキシ再暗号化方式は、ファイル共有システムに好適である。

先行技術文献

非特許文献

- [0013] 非特許文献1: B. Libert and D. Vergnaud, "Unidirectional Chosen-Cipher text Secure Proxy Re-encryption", Proc. PKC 2008, LNCS 4939, pp.360-379, Springer, 2008.

発明の概要

発明が解決しようとする課題

- [0014] しかしながら、(3)のプロキシ再暗号化方式では、サーバとユーザが結託した場合、復号権限を移譲元の許可なく再移譲されてしまうという不都合がある。具体的には、サーバ、ユーザB及びユーザEが結託した場合、ユーザA向けの暗号文をユーザB向けの暗号文に再暗号化するための再暗号化鍵 ($r k_{A \rightarrow B}$)、ユーザBの秘密鍵 ($s k_B$)、及びユーザEの秘密鍵 ($s k_E$) を用いて、ユーザA向けの暗号文をユーザE向けの暗号文に再暗号化するための正規の再暗号化鍵 ($r k_{A \rightarrow E}$) を、移譲元であるユーザAの許可なく計算できてしまう。

- [0015] 本発明が解決しようとする課題は、サーバとユーザが結託した場合でも、復号権限が移譲元の許可なく再移譲されることを阻止し得る再暗号化鍵生成装置、再暗号化装置及びプログラムを提供することである。

課題を解決するための手段

- [0016] 実施形態の再暗号化鍵生成装置は、第1ユーザ装置の第1公開鍵により平文データを暗号化して得られた暗号文データを復号せずに再暗号化して、第2ユーザ装置の第2秘密鍵により復号可能な再暗号文データを取得するための再暗号化鍵を生成する。
- [0017] 前記再暗号化鍵生成装置は、第1記憶手段、第2記憶手段、第1乱数生成手段及び再暗号化鍵生成手段を備えている。
- [0018] 前記第1記憶手段は、前記第1公開鍵に対応する第1秘密鍵を記憶する。
- [0019] 前記第2記憶手段は、前記第2秘密鍵に対応する第2公開鍵を記憶する。

[0020] 前記第 1 乱数生成手段は、第 1 乱数を生成する。

[0021] 前記再暗号化鍵生成手段は、前記第 1 秘密鍵、前記第 2 公開鍵及び前記第 1 乱数に基づいて、前記再暗号化鍵を生成する。

図面の簡単な説明

[0022] [図1]図 1 は、第 1 の実施形態に係る再暗号化システムの構成を示す模式図である。

[図2]図 2 は、同実施形態における鍵セットアップ処理の動作を説明するためのシーケンス図である。

[図3]図 3 は、同実施形態における暗号化処理の動作を説明するためのシーケンス図である。

[図4]図 4 は、同実施形態における再暗号化鍵生成処理の動作を説明するためのシーケンス図である。

[図5]図 5 は、同実施形態における再暗号化処理の動作を説明するためのシーケンス図である。

[図6]図 6 は、同実施形態における復号処理の動作を説明するためのシーケンス図である。

[図7]図 7 は、同実施形態に係るファイル共有システムの構成を例示する図である。

[図8]図 8 は、同実施形態におけるファイル共有システムの模式図である。

発明を実施するための形態

[0023] 以下、各実施形態について図面を用いて説明する。なお、以下の各装置は、それぞれハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、図 1 に示す如き、予めネットワーク又は非一時的なコンピュータ読取可能な記憶媒体 (non-transitory computer-readable storage medium) M 1 ~ M 5 からコンピュータにインストールされ、当該コンピュータのプロセッサに実行されることにより、当該コンピュータに各装置の機能を実現させるためのプログラムが用いられる。

[0024] (第1の実施形態)

始めに、プロキシ再暗号化方式について説明する。プロキシ再暗号化方式の基本的なモデルは以下の鍵生成、暗号化、復号、再暗号化鍵生成、再暗号化の5つの関数（以下、アルゴリズムともいう）からなる。鍵生成、暗号化、復号の機能は通常の公開鍵暗号と同様である。

[0025] (鍵生成) $\text{KeyGen}(1^k) \rightarrow (pk, sk)$

鍵生成アルゴリズムKeyGenは、セキュリティパラメータ 1^k が入力されると、公開鍵 pk と秘密鍵 sk の組 (pk, sk) を出力する。

[0026] (暗号化) $\text{Enc}(pk_A, m) \rightarrow C_A$

暗号化アルゴリズムEncは、ユーザAの公開鍵 pk_A とメッセージ m が入力されると、ユーザA宛の暗号文 C_A を出力する。

[0027] (復号) $\text{Dec}(sk_A, C_A) \rightarrow m$

復号アルゴリズムDecは、ユーザAの秘密鍵 sk_A と、ユーザA宛の暗号文 C_A とが入力されると、メッセージ m を出力する。

[0028] (再暗号化鍵生成) $\text{ReKeyGen}(pk_A, sk_A, pk_B, sk_B) \rightarrow rk_{A \rightarrow B}$

再暗号化鍵生成アルゴリズムReKeyGenは、ユーザAの公開鍵 pk_A 、ユーザAの秘密鍵 sk_A 、ユーザBの公開鍵 pk_B 、ユーザBの秘密鍵 sk_B が入力されると、再暗号化鍵 $rk_{A \rightarrow B}$ を出力する。

[0029] (再暗号化) $\text{ReEnc}(rk_{A \rightarrow B}, C_A) \rightarrow C_B$

再暗号化アルゴリズムReEncは、再暗号化鍵 $rk_{A \rightarrow B}$ と、ユーザA宛の暗号文 C_A とが入力されると、ユーザB宛の暗号文 C_B を出力する。

[0030] 以上が基本的なモデルである。但し、再暗号化の実現方式に応じて、関数への入力異なるモデルや、上記以外の関数や鍵を含むモデルも考えられている。

[0031] 例えば、本実施形態に示す再暗号化方式のように、再暗号化鍵生成アルゴリズムの入力において、ユーザBの秘密鍵 sk_B を不要とした非相互作用的 (non-interactive) と呼ばれるモデルが考えられている。また、ユーザAの秘密鍵 sk_A に代えて、ユーザB宛の再暗号化鍵 $rk_{A \rightarrow B}$ とユーザCの秘密鍵 sk_C

とが入力されるモデルなども考えられている。

[0032] また、再暗号化鍵 $r k_{A \rightarrow B}$ で暗号文 $C_A \rightarrow C_B$ の再暗号化を行える一方で、その逆の暗号文 $C_B \rightarrow C_A$ の変換を行えない一方向性 (unidirectional) と呼ばれるモデル、逆の変換も行える双方向性 (bidirectional) と呼ばれるモデルなども知られている。なお、双方向性モデルでは、再暗号化鍵 $r k_{A \rightarrow B}$ を $r k_{A \leftrightarrow B}$ と表すことがある。

[0033] さらに、公開鍵暗号の中でも ID ベース暗号に基づく方式も考えられている。その場合、マスター鍵生成のための関数セットアップ (Setup) が増え、鍵生成アルゴリズム KeyGen の入力にマスター鍵と ID が追加される。ID ベース暗号において、公開鍵 $p k$ は ID そのものである。

[0034] 次に、本実施形態に係るファイル共有システムの構成について図 7 を用いて説明する。ファイル共有システムは、サービスを提供するサービス提供者の有する情報処理装置であるサーバ S_v と、当該サービスの利用者であるユーザの有する情報処理装置であるユーザ装置 $A, B, C, \dots$ とを備えている。サーバ S_v と、ユーザ装置 $A, B, C, \dots$ とは通信網を介して接続されている。通信網とは、例えば、無線 LAN (Local Area Network)、有線 LAN、光回線網、電話回線網、イントラネット、イーサネット (登録商標) 及びインターネットやこれらの組み合わせである。尚、同図では、ファイル共有システムに接続されるサーバ S_v は 1 台のみが示されているが、複数台であっても良い。また、ユーザ装置 $A, B, C, \dots$ は、ユーザ $A, B, C, \dots$ と略記する場合や、第 1 ユーザ装置、第 2 ユーザ装置、 $\dots$ と呼ぶ場合がある。

[0035] 図 8 は、ファイル共有システムの模式図である。このファイル共有システムは、サーバ S_v 、ユーザ A 、ユーザ B 、ユーザ C 、グループ管理者、及びユーザ管理者からなる。ユーザ管理者とは、全ユーザを管理するエンティティである。ユーザ管理者は、ユーザがファイル共有システムにログインできるようにするための ID と初期パスワードを各ユーザに対して発行する。

[0036] 事前準備として、各ユーザは、グループ管理者の公開鍵 $p k_{Gr}$ を持っている

ものとする。また、共有しようとする平文のファイルデータを m と表記する。サーバ S_v は、グループ管理者宛の暗号文 $E(p k_{Gr}, m)$ をユーザ A （又はユーザ B 、又はユーザ C ）宛の暗号文 $E(p k_A, m)$ （又は $E(p k_B, m)$ ）、又は $E(p k_C, m)$ ）に再暗号化する再暗号化鍵 $r k_{Gr \rightarrow A}$ （又は $r k_{Gr \rightarrow B}$ 、又は $r k_{Gr \rightarrow C}$ ）を持っているものとする。各ユーザ i は秘密鍵 $s k_i$ を持っているものとする。つまり、ユーザ A は秘密鍵 $s k_A$ 、ユーザ B は $s k_B$ 、ユーザ C は $s k_C$ をそれぞれ持っている。

[0037] 次に、ユーザ C は、公開鍵記憶部1に記憶されているグループ管理者の公開鍵 $p k_{Gr}$ でファイルデータ m を暗号化し、得られた暗号文 $E(p k_{Gr}, m)$ をサーバ S_v へアップロードする。サーバ S_v は、暗号文記憶部2においてこの暗号文を保管する。

[0038] 今、ユーザ A がファイルデータ m を共有したいとする。ユーザ A は、サーバ S_v に対して暗号文 $E(p k_{Gr}, m)$ の再暗号化の要求を送信する。サーバ S_v は、ユーザ A から受けた要求に対し、再暗号化鍵記憶部3に記憶されているユーザ A 宛の再暗号化鍵 $r k_{Gr \rightarrow A}$ に基づいて、暗号文 $E(p k_{Gr}, m)$ をユーザ A 宛の再暗号文 $E(p k_A, m)$ に再暗号化し、得られた再暗号文 $E(p k_A, m)$ をユーザ A に送信する。ここで、再暗号文とは、暗号文を再暗号化した暗号文である。

[0039] ユーザ A は、サーバ S_v からダウンロードした再暗号文 $E(p k_A, m)$ を自身が保有する秘密鍵 $s k_A$ で復号し、得られたファイルデータ m を利用する。

[0040] 以上のようなファイル共有システムは、ユーザ C による暗号化からユーザ A による復号までの間、ファイルデータ M が一度も復号されないため、ファイル共有の過程における情報の漏洩を阻止することができる。

[0041] また、ユーザ C は、暗号文をアップロードする時点で、どのユーザとファイル共有するかを決定する必要がない。つまり、ユーザ C は、ファイルデータ m をグループ管理者の公開鍵 $p k_{Gr}$ で暗号化すれば良く、暗号化に関して管理すべき鍵がグループ管理者の公開鍵 $p k_{Gr}$ のみで良いので、鍵管理のコスト

を低減させることができる。

[0042] 本ファイル共有システムにおいて、サーバS_vは、暗号文E (p k_{Gr}, m)を復号するための復号鍵s k_{Gr}を持たない。従って、サーバS_vはこの暗号文を復号できない。これは、不正なサーバS_vが暗号文を復号して漏洩させてしまうといった脅威を排除できるため、サーバS_vを厳重に管理しなくても良く、サーバS_vの管理コストの低減に繋がる。

[0043] ユーザBがファイル共有を行う際も上記と同様である。

[0044] 図1は第1の実施形態に係る再暗号化システムの構成を示す模式図である。(図1と図8の対応関係については後述する。)この再暗号化システムは、鍵生成装置10、暗号化装置20、再暗号化鍵生成装置30、再暗号化装置40及び復号装置50を備えている。ここで、鍵生成装置10は、再暗号化システムの各種パラメータ及び各装置40、50の公開鍵・秘密鍵のペアを生成する。

[0045] 暗号化装置20は、再暗号化鍵生成装置30の秘密鍵に対応する公開鍵を用いて平文データを暗号化して得られた暗号文データを再暗号化装置40に送信する。

[0046] 再暗号化鍵生成装置30は、再暗号化鍵生成装置30の秘密鍵と復号装置50の公開鍵と乱数とを用いて再暗号化鍵を生成する。

[0047] 再暗号化装置40は、暗号化装置20から受けた暗号文データを復号せずに再暗号化鍵により再暗号化して得られた再暗号文データを復号装置50に送信する。

[0048] 復号装置50は、再暗号化鍵生成装置30の公開鍵を用いて再暗号文データを検証処理すると共に、自装置50の公開鍵に対応する秘密鍵を用いて再暗号文データを復号処理して平文データを得る。なお、再暗号化鍵生成装置30、再暗号化装置40及び復号装置50は、それぞれ複数台が設けられていてもよいが、ここでは一台ずつ設けられている場合を例に挙げて述べる。

[0049] 図1と図8の対応関係について説明する。各装置10～50は、当該処理を行うエンティティにより保持される。ユーザが自身の公開鍵と秘密鍵の組

を生成する場合、当該ユーザは鍵生成装置 10 を保持する。なお、例えば、ユーザ管理者又はグループ管理者がユーザの公開鍵と秘密鍵の組を生成する場合、ユーザ管理者又はグループ管理者が鍵生成装置 10 を保持する。ユーザは、暗号化装置 20、復号装置 50、又は両方を保持する。グループ管理者は、再暗号化鍵生成装置 30 を保持する。なお、例えば、ユーザ管理者又はサーバ S v が再暗号化鍵を生成する場合、ユーザ管理者又はサーバ S v が再暗号化鍵生成装置 30 を保持する。サーバ S v は、再暗号化装置 40 を保持する。図 8 に例示したファイル共有システムにおいては、サーバ S v が公開鍵記憶部 1 を保持し、暗号化を行うユーザ C は、公開鍵記憶部 1 から暗号化に用いる公開鍵を取得しているが、これに限らず、後述するように、ユーザ C は（暗号化に用いる公開鍵を生成した）鍵生成装置 10 から暗号化に用いる公開鍵を取得しても良い。また、サーバ S v は、ユーザ C が生成した暗号文 $E(p k_{Gr}, m)$ を暗号文記憶部 2 において保管するが、暗号文記憶部 2 は再暗号化装置 40 に含まれていても良いし、再暗号化装置 40 に含まれない外部の記憶装置であっても良い。

[0050] どのエンティティがどの装置を保持するかについては、上述の例に限定されるものではなく、様々なバリエーションが考えられる。また、ユーザ管理者又はグループ管理者がユーザを兼ねる場合も兼ねない場合もある。また、各ユーザが用いる各ユーザ装置は、第 1 ユーザ装置、第 2 ユーザ装置、…と呼んでもよい。同様に、各ユーザ装置の公開鍵及び秘密鍵は、第 1 ユーザ装置の第 1 公開鍵及び第 1 秘密鍵、第 2 ユーザ装置の第 2 公開鍵及び第 2 秘密鍵、…と呼んでもよい。

[0051] 続いて、各装置 10～50 の構成を具体的に説明する。

[0052] 鍵生成装置 10 は、鍵生成パラメータ記憶部 11、一時データ記憶部 12、公開パラメータ生成部 13、公開鍵・秘密鍵生成部 14、通信部 15 及び制御部 16 を備えている。

[0053] ここで、鍵生成パラメータ記憶部 11 は、鍵生成パラメータを記憶する記憶装置である。

- [0054] 一時データ記憶部 12 は、各生成部 13, 14 の処理途中及び処理結果などの一時データを記憶する記憶装置である。
- [0055] 公開パラメータ生成部 13 は、鍵生成の公開パラメータを生成する。
- [0056] 公開鍵・秘密鍵生成部 14 は、ユーザ宛の公開鍵・秘密鍵を生成する。
- [0057] 通信部 15 は、他の装置 20～50 と通信するための通信インタフェースであり、例えば、以下の各機能(f15-1)～(f15-2)をもっている。
- [0058] (f15-1) 制御部 16 に制御されて一時データ記憶部 12 内の各 30, 50 の公開鍵・秘密鍵のペアを当該各装置 30, 50 に送信する機能。
- [0059] (f15-2) 制御部 16 に制御されて一時データ記憶部 12 内の再暗号化鍵生成装置 30 の公開鍵を暗号化装置 20 に送信する機能。
- [0060] なお、以下の説明では、送受信時の冗長な記載を避ける観点から、送受信の際に、通信部 15 を介する旨の記載を省略する場合がある。これは他の装置 20～50 の通信部についても同様である。
- [0061] 制御部 16 は、図 2 に示す動作を実行するように、各部 11～15 を制御する機能をもっている。
- [0062] 暗号化装置 20 は、一時データ記憶部 21、通信部 22、暗号化データ生成部 23、暗号文生成部 24 及び制御部 25 を備えている。
- [0063] ここで、一時データ記憶部 21 は、鍵生成装置 10 から受けた再暗号化鍵生成装置 30 の公開鍵や、各生成部 23, 24 の処理途中及び処理結果などの一時的なデータ（以下、一時データともいう）を記憶する記憶装置である。
- [0064] 通信部 22 は、他の装置 10, 30～50 と通信するための通信インタフェースであり、例えば、以下の各機能(f22-1)～(f22-2)をもっている。
- [0065] (f22-1) 鍵生成装置 10 に公開された再暗号化鍵生成装置 30 の公開鍵を取得して一時データ記憶部 21 に書き込む機能。
- [0066] (f22-2) 制御部 25 に制御されて一時データ記憶部 21 内の暗号文データを再暗号化装置 40 に送信する機能。
- [0067] 暗号化パラメータ生成部 23 は、暗号化パラメータを生成する機能をもつ

ている。

[0068] 暗号文生成部 24 は、例えば、以下の各機能 (f24-1) ~ (f24-2) をもっている。

[0069] (f24-1) 一時データ記憶部 21 から読み出した再暗号化鍵生成装置 30 の公開鍵 (第 1 ユーザ装置の第 1 公開鍵) を用いて平文データを暗号化することにより、暗号文データを生成する機能。

[0070] (f24-2) 得られた暗号文データを一時データ記憶部 21 に書き込む機能。

[0071] 制御部 25 は、図 3 に示す動作を実行するように、各部 21 ~ 24 を制御する機能をもっている。

[0072] 再暗号化鍵生成装置 30 は、秘密鍵記憶部 31、一時データ記憶部 32、通信部 33、再暗号化鍵生成部 34、制御部 35 及び乱数生成部 36 を備えている。

[0073] 秘密鍵記憶部 31 は、鍵生成装置 10 から受けた再暗号化鍵生成装置 30 の秘密鍵を記憶する記憶装置である。

[0074] 一時データ記憶部 32 は、鍵生成装置 10 から受けた復号装置 50 の公開鍵や、再暗号化鍵生成部 34 の処理途中及び処理結果などの一時データを記憶する記憶装置である。

[0075] 通信部 33 は、他の装置 10, 20, 40, 50 と通信するための通信インタフェースであり、例えば制御部 35 に制御されて一時データ記憶部 32 内の再暗号化鍵を再暗号化装置 40 に送信する機能をもっている。

[0076] 再暗号化鍵生成部 34 は、例えば、以下の各機能 (f34-1) ~ (f34-2) をもっている。

[0077] (f34-1) 秘密鍵記憶部 31 から読み出した再暗号化鍵生成装置 30 の秘密鍵 (第 1 ユーザ装置の第 1 秘密鍵) と、一時データ記憶部 32 から読み出した復号装置 50 の公開鍵 (第 2 ユーザ装置の第 2 公開鍵) と、乱数生成部 36 により生成された乱数とに基づいて再暗号化鍵を生成する機能 (この機能では暗号化時のパラメータ詳しくは乱数一が不要)。

[0078] (f34-2) この再暗号化鍵を一時データ記憶部 32 に書き込む機能。

- [0079] 制御部 35 は、図 4 に示す動作を実行するように、各部 31～34, 36 を制御する機能をもっている。
- [0080] 乱数生成部 36 は、乱数を生成して再暗号化鍵生成部 34 に送出する機能をもっている。
- [0081] 再暗号化装置 40 は、再暗号化鍵記憶部 41、一時データ記憶部 42、通信部 43、再暗号化処理部 44、再暗号化パラメータ生成部 45 及び制御部 47 を備えている。
- [0082] 再暗号化鍵記憶部 41 は、再暗号化鍵生成装置 30 から受けた再暗号化鍵を記憶する記憶装置である。
- [0083] 一時データ記憶部 42 は、再暗号化処理部 44 の処理途中及び処理結果などの一時データを記憶する記憶装置である。
- [0084] 通信部 43 は、他の装置 10～30, 50 と通信するための通信インタフェースであり、例えば、以下の各機能(f43-1)～(f43-2)をもっている。
- [0085] (f43-1) 暗号化装置 20 から受けた暗号文データを再暗号化処理部 44 に送出する機能。
- [0086] (f43-2) 制御部 47 に制御されて一時データ記憶部 42 内の再暗号文データを復号装置 50 に送信する機能。
- [0087] 再暗号化処理部 44 は、例えば、以下の各機能(f44-1)～(f44-2)をもっている。
- [0088] (f44-1) 暗号化装置 20 から暗号文データを受けると、再暗号化鍵記憶部 41 から読み出した再暗号化鍵を用いて当該暗号文データを復号せずに再暗号化することにより、再暗号文データを得る機能。
- [0089] (f44-2) 得られた再暗号文データを一時データ記憶部 42 に書き込む機能。
- [0090] 制御部 47 は、再暗号文検証プログラムを配信する動作（図示せず）と図 5 に示す動作を実行するように、各部 41～45 を制御する機能をもっている。
- [0091] 復号装置 50 は、秘密鍵記憶部 51、一時データ記憶部 52、通信部 53

、復号処理部 5 4、及び制御部 5 6 を備えている。

[0092] 秘密鍵記憶部 5 1 は、鍵生成装置 1 0 から受けた自装置 5 0 の秘密鍵を記憶する記憶装置である。

[0093] 一時データ記憶部 5 2 は、鍵生成装置 1 0 から受けた自装置 5 0 の公開鍵及び再暗号化鍵生成装置 3 0 の公開鍵や、復号処理部 5 4 の処理途中及び処理結果などの一時データを記憶する記憶装置である。

[0094] 通信部 5 3 は、他の装置 1 0 ～ 4 0 と通信するための通信インタフェースであり、例えば、以下の各機能(f53-1)～(f53-3)をもっている。

[0095] (f53-1) 鍵生成装置 1 0 から受けた自装置 5 0 の秘密鍵を秘密鍵記憶部 5 1 に書き込む機能。

[0096] (f53-2) 鍵生成装置 1 0 から受けた自装置 5 0 の公開鍵及び再暗号化鍵生成装置 3 0 の公開鍵を一時データ記憶部 5 2 に書き込む機能。

[0097] (f53-3) 再暗号化装置 4 0 から受けた再暗号化データを復号処理部 5 4 に送出する機能。

[0098] 復号処理部 5 4 は、例えば、以下の各機能(f54-1)～(f54-3)をもっている。

[0099] (f54-1) 再暗号化装置 4 0 から再暗号文データを受けると、秘密鍵記憶部 5 1 から読み出した当該復号装置 5 0 の秘密鍵（第 2 ユーザ装置の第 2 秘密鍵）に基づいて、当該再暗号文データを復号処理することにより、平文データを得る機能。

[0100] (f54-2) 得られた平文データを一時データ記憶部 5 2 に書き込む機能。

[0101] 制御部 5 6 は、図 6 に示す動作を実行するように、各部 5 1 ～ 5 4 を制御する機能をもっている。

[0102] 次に、以上のように構成された再暗号化システムの動作を図 2 乃至図 6 のシーケンス図を用いて説明する。

[0103] また、以下の動作は（１）鍵セットアップ処理、（２）暗号化処理、（３）再暗号化鍵生成処理、（４）再暗号化処理、（５）復号処理の手順で実行される場合を例に挙げて述べる。但し、以下の動作は、必ずしも上記手順で

処理を実行しなくてもよい。例えば、再暗号化鍵生成は、暗号化処理の前に実行されてもよい。また、再暗号化処理が実行されずに、暗号文データが復号されてもよい。

[0104] (1) 鍵セットアップ処理は、鍵生成装置 10 により、図 2 及び以下の各ステップ S T 1 ~ S T 12 に示すように実行される。

[0105] 始めに、鍵生成装置 10 の公開パラメータ生成部 13 は、公開パラメータ ($p, \lambda, G, G_T, g, g_1, g_2, u, v,$
[数1]

$$\text{Sig}(\hat{G}, \hat{S}, \hat{V})$$

[0106]) を生成する、又は外部から入手する (S T 1)。具体的には、公開パラメータ生成部 13 は、予め鍵パラメータ記憶部 11 に記憶したセキュリティパラメータ λ に基づいて、素数位数 $p > 2^\lambda$ を満たす双線型写像群 (bilinear map groups) (G, G_T)、 G の元 g, g_1, g_2, u, v 、強偽造不可能性を満たす使い捨て署名 (one-time signature) アルゴリズム
[数2]

$$\text{Sig}(\hat{G}, \hat{S}, \hat{V})$$

[0107] を生成する。なお、 Z_p^* は Z_p から p と互いに素な整数の集合 ($= (Z/pZ)^*$) であり、素数 p に対する乗法群 Z_p^* と呼んでもよい。 Z_p は 0 以上 p 未満の整数の集合 ($= (Z/pZ)$) である。そして、「元」(げん)とは、数学的な意味を持つ用語であり、要素とも呼ばれ、複数の「もの」で構成されている集合の中において、集合を構成している個々のものを指す。また、使い捨て署名アルゴリズム
[数3]

$\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ (以下、 $\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ を sig ともいう) における $\hat{G}$ は使い捨ての鍵ペア ($s s k, s v k$) を生成する機能を意味し、 $\hat{S}$ はメッセージ M に対する署名 σ を生成する機能を意味し、 $\hat{V}$ は署名 σ の正当性を検証する機能を意味する。

[0108] 使い捨て署名については、A. Menezes, P. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, (1996) pp.462-471, (1996)に詳しい。

[0109] また、双線型写像 (e と表記する) とは、 $e : G \times G \rightarrow G_T$ となる写像であり、以下の3つの性質を満たす。

[0110] 1. 任意の $(g, h) \in G \times G$ 及び $a, b \in \mathbb{Z}$ について、 $e(g^a, h^b) = e(g, h)^{a \cdot b}$ が成り立つ。ここで、 $\mathbb{Z}$ とは整数の集合である。

[0111] 2. 任意の $(g, h) \in G \times G$ について、 $e(g, h)$ が計算可能である。

[0112] 3. $g, h \neq 1_G$ である場合は常に $e(g, h) \neq 1_{G_T}$ が成り立つ。ここで、 1_G とは G の単位元であり、 1_{G_T} とは G_T の単位元である。

[0113] また、双線型写像群(bilinear map groups) (G, G_T と表記する) とは、双線型写像 $e : G \times G \rightarrow G_T$ が存在する素数位数 p の群である。上記の定義は、 G の元 g, g_1, g_2 について、 $g_1 = g^\alpha, g_2 = g^\beta$ とすると、次式が成り立つことも意味する (但し、 α, β は、 G の元 g, g_1, g_2 に関するべき指数である)。

[0114]
$$e(g_1 g_2, g) = e(g, g_1 g_2) = e(g, g^\alpha \cdot g^\beta) = e(g, g^{\alpha + \beta}) = e(g, g)^{\alpha + \beta} = e(g, g)^\alpha \cdot e(g, g)^\beta$$

なお、 G の複数の元 g, g_1, g_2 は、予め定められた複数のシステム固定値となっている。複数のシステム固定値としては、双線型写像群 G の3つの元に限らず、 G の2つ又は4つ以上といった複数の元が適宜使用可能となっている。また、「システム固定値」の語は、「固定値」、「元」又は「システムパラメータ」などと読み替えてもよい。この複数のシステム固定値は、双線型写像が存在する素数位数の群である双線型写像群の複数の元である。

[0115] また、本明細書では、 G, G_T をともに乗法群と想定した記法を採用しているが、これに限らず、 G, G_T それぞれについて、加法群と想定した記法で表すことも可能である。つまり、例えば、 G を加法群、 G_T を乗法群として表現しても良い。また、双線型写像として、双線型写像群 G_1, G_2, G_T (G_1 と G_2 は異なる群である) について、 $e : G_1 \times G_2 \rightarrow G_T$ となる写像を用いても良い。

これらは他の実施形態においても同様である。

[0116] 続いて、公開パラメータ生成部 13 は、生成した公開パラメータを一時データ記憶部 12 に書き込む。鍵生成装置 10 は、一時データ記憶部 12 内の公開パラメータ $p, \lambda, G, G_1, g, g_1, g_2, u, v, \text{Sig}$ を公開する (ST2)。なお、スツツ ST1 を実行する前に公開パラメータが既に公開されていた場合、その公開パラメータを一時データ記憶部 12 に書き込み、スツツ ST1 及びスツツ ST2 をスキップしても良い。

[0117] また、公開鍵・秘密鍵生成部 14 は、再暗号化鍵生成装置 30 の識別情報を！としたとき、再暗号化鍵生成装置 30 の秘密鍵 $x_i, y_i, z_i \in Z_p^*$ を生成し、この秘密鍵 $s_{k_i} = (x_i, y_i, z_i)$ を用いて再暗号化鍵生成装置 30 の公開鍵

[数4]

$$pk_i = (X_i, Y_i, Z_i, Z_{1i})$$

を生成する (ST7)。ここで、

$$X_i = g^{x_i}, Y_i = g^{y_i}, Z_i = g^{z_i}, Z_{1i} = g^{z_i}$$

[0118] である。

[0119] 続いて、公開鍵・秘密鍵生成部 14 は、生成した公開鍵・秘密鍵のペアを一時データ記憶部 12 に書き込む。通信部 15 は、制御部 16 に制御されて一時データ記憶部 12 内の秘密鍵 s_{k_i} を再暗号化鍵生成装置 30 に送信する (ST8)。鍵生成装置 10 は、一時データ記憶部 12 内の再暗号化鍵生成装置 30 の公開鍵 pk_i を公開する (ST9)。

[0120] また同様に、公開鍵・秘密鍵生成部 14 は、復号装置 50 の識別情報を！としたとき、復号装置 50 の秘密鍵 $s_{k_j} = (x_j, y_j, z_j)$ を生成し、この秘密鍵 s_{k_j} を用いて復号装置 50 の公開鍵

[数5]

$$pk_j = (X_j, Y_j, Z_j, Z_{ij})$$

を生成する (ST10)。ここで、

$$X_j = g^{x_j}, Y_j = g^{y_j}, Z_j = g^{z_j}, Z_{ij} = g^{z_{ij}}$$

[0121] である。

[0122] 続いて、公開鍵・秘密鍵生成部14は、生成した公開鍵・秘密鍵のペアを

一時データ記憶部12に書き込む。通信部15は、制御部16に制御されて

一時データ記憶部12内の秘密鍵 s_j を復号装置50に送信する (ST11

)。鍵生成装置10は、一時データ記憶部12内の復号装置50の公開鍵 p

k_j を公開する (ST12)。また、所望により、暗号化装置20の秘密鍵 s

k_h 及び公開鍵 $p k_h$ についても各スロットST10～ST12と同様の処理を

実行して暗号化装置20に秘密鍵 $s k_h$ を送信し、公開鍵 $p k X_h$ を公開しても

よい。

[0123] 以上により、鍵セットアップ処理が完了する。以後、各装置20、30、

40、50では、各スロットST2、ST6、ST9、ST12で公開され

た公開パラメータ及び公開鍵を適宜、取得して利用することができる。

[0124] (2) 暗号化処理は、暗号化装置20により、図3及び以下の各スロット

ST21～ST24に示すように実行される。

[0125] すなわち、暗号化装置20の暗号化パラメータ生成部23は、公開パラメ

ータにおけるセキュリティパラメータ λ 及び鍵ペア生成機能

[数6]

$\hat{G}$ を用いて、使い捨て署名における署名鍵 $s k$ と検証鍵 $s v k$ の鍵ペア

$$(s k, s v k) = \hat{G}(\lambda)$$

[0126] を生成し (ST21)、暗号化データ C_1 に検証鍵 $s v k$ をセットする ($C_1 =$

$s v k$)。

[0127] また、暗号化パラメータ生成部23は、乱数 $r \in Z_p^*$ を生成して暗号文生成

部24に送出する。

[0128] 暗号文生成部 24 は、この乱数 r 及び再暗号化鍵生成装置 30 の公開鍵 p k_i を用いて、平文データとしてのメッセージ $m \in G_1$ に対して、以下の暗号化データ $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4$ を生成する (S T 22)。

[数7]

$$C_{2X} = X_i^T, C_{2Y} = Y_{i1}^T, C_{2Z} = Z_i^T, C_{2Z1} = Z_{i1}^T, \\ C_3 = e(g_1 g_2, g)^T \cdot m, C_4 = (u^{sk} \cdot v)^T$$

スレッド S T 22 の終了後、暗号文生成部 24 は、暗号化データ C_3, C_4 に対し、公開パラメータにおける署名生成機能 $\$$ とスレッド S T 21 で生成した署名鍵 $s k$ による使い捨て署名 σ を次式に示すように生成する (S T 23)。

$$\sigma = \$ (s k, (C_3, C_4))$$

[0129] しかる後、暗号文生成部 24 は、上記全ての暗号化データ $C_1 \sim C_4$ と使い捨て署名 σ とを含む暗号文データ $C_i = (C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部 21 に書き込む。

なお、暗号文データ $C_i = (C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, \sigma)$ は、検証を省略する場合、復号に用いない検証用データ (C_1, C_4, σ) を省略して、 $C_i = (C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)$ としてもよい。この場合、検証用データ (C_1, C_4, σ) を生成する処理も省略される。

[0130] いずれにしても通信部 22 は、制御部 25 に制御されて一時データ記憶部 21 内の暗号文データ C_i を再暗号化装置 40 に送信する (S T 24)。

[0131] 以上により、暗号化処理が完了する。

[0132] なお、本実施形態においては、上述したように (また後述するように) 検証を省略したり、検証用データの生成を省略したりしてもよいが、これは後述する実施形態や変形例においても同様である。

[0133] (3) 再暗号化鍵生成処理は、再暗号化鍵生成装置 30 により、図 4 及び以下の各スレッド S T 31 ~ S T 33 に示すように実行される。

[0134] すなわち、再暗号化鍵生成装置 30 の通信部 33 は、制御部 35 に制御されて、鍵生成装置 10 から公開された復号装置 50 の公開鍵 $p k_j$ を取得して一時データ記憶部 32 に書き込む (S T 31)。また、通信部 33 は、前述

したスツツPT5のとき、再暗号化鍵生成装置30の秘密鍵 s_k を鍵生成装置10から受信して秘密鍵記憶部31に書き込んでいる。

- [0135] 乱数生成部36は、乱数 $\theta \in \mathbb{Z}_p^*$ を生成して再暗号化鍵生成部34に送出する。
- [0136] 再暗号化鍵生成部34は、この乱数 θ 、秘密鍵記憶部31内の再暗号化鍵生成装置30の秘密鍵 s_k 、及び一時データ記憶部32内の復号装置50の公開鍵 p_{k_j} に基づいて、再暗号化鍵 R_{ij} を次式に示すように生成する (ST32)。

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

ここで、

$$R_{ij1} = (X_j \cdot g^{\theta})^{1/x_i} = g^{\frac{x_j + \theta}{x_i}}, R_{ij2} = (Y_{z_j} \cdot g^{\theta})^{1/y_i} = g^{\frac{y_{z_j} + \theta}{y_i}}, R_{ij3} = (X_j \cdot Y_{z_j} \cdot g^{\theta})^{1/z_i} = g^{\frac{x_j + y_{z_j} + \theta}{z_i}}.$$

[0137] である。なお、上式では、 $g^1 = g^a$ 、 $g^2 = g^b$ と書き替えて表記している。

- [0138] しかる後、再暗号化鍵生成部34は、生成した再暗号化鍵 R_{ij} を一時データ記憶部32に書き込む。通信部33は、制御部35に制御されて、一時データ記憶部32内の再暗号化鍵 R_{ij} を再暗号化装置40に送信する (ST33)。

[0139] 以上により、再暗号化鍵生成処理が完了する。

- [0140] (4) 再暗号化処理は、再暗号化装置40により、図5及び以下の各スツツPT41～ST43に示すように実行される。

- [0141] 再暗号化装置40の通信部43は、スツツPT24で送信された暗号文データ C_i と、スツツPT33で送信された再暗号化鍵 R_{ij} とをそれぞれ一時データ記憶部42に書き込む。

- [0142] 再暗号化処理部44は、公開パラメータと次の検証式を用い、一時データ記憶部42内の暗号文データ C_i を検証する (ST41)。

[数9]

$$\begin{aligned}
e(C_{2X}, u^{C_1} \cdot v) &= e(X_i, C_4) \\
e(C_{2Y}, u^{C_1} \cdot v) &= e(Y_{1i}, C_4) \\
e(C_{2Z}, u^{C_1} \cdot v) &= e(Z_i, C_4) \\
e(C_{2Z1}, u^{C_1} \cdot v) &= e(Z_{1i}, C_4) \\
V(C_1, \sigma, (C_3, C_4)) &= 1
\end{aligned}$$

[0143] ここで、上記5つの検証式が全て成立すれば検証は成功し、1つでも成立しない検証式があれば検証は失敗する。

[0144] 検証が成功した場合、再暗号化パラメータ生成部45は、3つの乱数 s , t , $k \in \mathbb{Z}_p^*$ を生成して再暗号化処理部44に送出する。

[0145] 再暗号化処理部44は、これらの乱数 s , t , k 、一時データ記憶部42内の暗号文データ C_i 、及び一時データ記憶部42内の再暗号化鍵 R_{ij} を用いて、次式に示すように、再暗号化データ C_{2X}' , C_{2X}'' , C_{2Y}' , C_{2Y}'' , C_{2Z}' , C_{2Z}'' , C_{2Z1}' , C_{2Z1}'' , $C_{2'}''$, C_{5X} , C_{5Y} , C_{5Z} を生成する (S T 4 2)。

[数10]

$$\begin{aligned}
C_{2X}' &= X_i^s, C_{2X}'' = C_{2X}^s = X_i^{rs}, C_{2Y}' = Y_{1i}^t, C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, \\
C_{2Z}' &= Z_i^k, C_{2Z}'' = C_{2Z}^k = Z_i^{rk}, C_{2Z1}' = Z_{1i}^k, C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk}, \\
C_{5X} &= R_{ij1}^{\frac{1}{s}}, C_{5Y} = R_{ij2}^{\frac{1}{t}}, C_{5Z} = R_{ij3}^{\frac{1}{k}}
\end{aligned}$$

[0146] ステップS T 4 2の終了後、再暗号化処理部44は、上記全ての暗号化データ再暗号化データ $C_{2X}' \sim C_{5Z}$ を、暗号文データ C_i 内の暗号化データ C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} と置換して再暗号文データ $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2'}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ を生成し、得られた再暗号文データ C_j を一時データ記憶部42に書き込む。なお、再暗号文データ $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2'}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ は、検証を省略する場合、復号に用いない検証用データ ($C_1, C_{2X}', C_{2Y}', C_{2Z}'$

, C_{2Z1}' , $C_{2'}''$, C_4 , σ) を省略して、 $C_j = (C_{2X}'', C_{2Y}'', C_{2Z}'', C_{2Z1}'', C_{5X}', C_{5Y}', C_{5Z}', C_3)$ としてもよい。この場合、検証用データ (C_{2X}' , C_{2Y}' , C_{2Z}' , C_{2Z1}' , $C_{2'}''$) を生成する処理も省略される。

[0147] いずれにしても通信部 43 は、制御部 47 に制御されて一時データ記憶部 42 内の再暗号文データ C_j を復号装置 50 に送信する (ST43)。

[0148] 以上により、再暗号化処理が完了する。

[0149] (5) 復号処理は、復号装置 50 により、図 6 及び以下のステップ ST51 及び ST52 に示すように実行される。

[0150] すなわち、復号装置 50 の通信部 53 は、ステップ ST43 で送信された再暗号文データ C_j を受信して一時データ記憶部 52 に書き込む。

[0151] 復号処理部 54 は、公開パラメータ及び自装置 50 の公開鍵 pk_j と次の検証式を用い、一時データ記憶部 52 内の再暗号文データ C_j を検証する (ST51)。

[数11]

$$\begin{aligned} e(C_{2X}'', u^{C_1} \cdot v) &= e(C_{2X}', C_4) \\ e(C_{2Y}'', u^{C_1} \cdot v) &= e(C_{2Y}', C_4) \\ e(C_{2Z}'', u^{C_1} \cdot v) &= e(C_{2Z}', C_4) \\ e(C_{2Z1}'', u^{C_1} \cdot v) &= e(C_{2Z1}', C_4) \\ e(C_{5Z}, C_{2Z}') &= e(C_{5X}, C_{2X}') \cdot e(Y_{2j}, g) \\ e(C_{5Z}, C_{2Z1}') &= e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_1) \\ \mathcal{V}(C_1, \sigma, (C_3, C_4)) &= 1 \end{aligned}$$

[0152] ここで、上記 7 つの検証式が全て成立すれば検証は成功し、1 つでも成立しない検証式があれば検証は失敗する。

[0153] 検証が成功した場合、復号処理部 54 は、自装置の秘密鍵 sk_j を用いて、次式に示すように、再暗号文データ C_j を復号し、メッセージ m を得る (ST52)。

[数12]

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\}$$

上式の復号結果がmとなることは、次式により確認できる。なお、次式では、 $g_1 = g^\alpha$, $g_2 = g^\beta$ と書き替えて表記している。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{(x_j + \beta y_j + \theta)/z_i k}, g^{z_i \tau k})}{e(g^{(x_j + \theta)/x_i s}, g^{x_i \tau s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(x_j + \beta y_j + \theta)/z_i k}, g^{\alpha z_i \tau k})}{e(g^{(\beta y_j + \theta)/y_i t}, g^{\alpha y_i \tau t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{x_j + \beta y_j + \theta}, g^r)}{e(g^{x_j + \theta}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{x_j + \beta y_j + \theta}, g^{\alpha r})}{e(g^{\beta y_j + \theta}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_1 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\alpha r}) = m. \end{aligned}$$

[0154] なお、復号処理部54は、ステップST51の検証処理を省略し、ステップST52の復号処理を行ってもよい。また、再暗号文データC_jに検証用データが含まれていない場合も、復号処理部54は、ステップST51の検証処理を省略し、ステップST52の復号処理を行う。また、上記mはメッセージそのものではなく、鍵であってもよい。例えば、共通鍵暗号における共通鍵keyについて、m=keyとして、mをkeyに置き換えてもよい。この場合、共通鍵keyを用いてメッセージを暗号化した暗号文を上記暗号文データや再暗号文データに付加すればよい。これらは後述する実施形態や変形例においても同様である。

[0155] なお、本実施形態は、適宜、処理の順番を変更してもよい。例えば、復号処理と暗号文検証処理の順番を変更してもよい。同様に、再暗号化鍵生成処理では暗号化処理を行なう際のパラメータ詳しくは乱数一が不要であるため、再暗号化鍵生成処理の順番を暗号化処理よりも前に変更してもよい。

[0156] 上述したように本実施形態によれば、再暗号化鍵R_{ij}を乱数θに基づいて生成する構成により、サーバとユーザが結託した場合でも、復号権限を移譲元の許可なく再移譲されることを防ぐことができる。また、これにより、サー

バに対して極端な信頼を求める必要が無くなるため、ユーザがより安心して利用できるファイル共有システムを提供することができる。

[0157] [変形例 1]

第 1 の実施形態では、暗号化装置 20 において暗号文データを生成し、再暗号化装置 40 において暗号文データを再暗号化して再暗号文データを生成し、復号装置 50 において再暗号文データを復号する例を挙げた。しかしながら、再暗号化せずに暗号文データを復号する形態に、第 1 の実施形態を変更しても良い。この場合、鍵セットアップ処理、暗号化処理、復号処理のみを行えば良い。本変形例における鍵セットアップ処理は、第 1 の実施形態における鍵セットアップ処理と同じである。以下、本変形例における暗号化処理及び復号処理について説明する。

[0158] 本変形例における暗号化処理と、第 1 の実施形態における暗号化処理との違いは、最終ステップのみである。前述の記号を流用して説明をするために、便宜上、復号装置 50 の識別情報を i とする。この場合、暗号化装置 20 の通信部 22 は、制御部 25 に制御されて一時データ記憶部 21 内の暗号文データ C_i を復号装置 50 に送信する (ST24')。

[0159] 復号装置 50 は、暗号化装置 20 において生成された暗号文データ C_i をステップ ST41 と同様に検証する。検証が成功した場合、復号装置 50 は、秘密鍵 s_{k_i} を用いて、次式のように暗号文データ C_i を復号し、メッセージ m を得る。

[数13]

$$m = C_3 / e(g_1 g_2, C_{2X})^{\frac{1}{x_i}}$$

上式の復号結果が m となることは、次式により確認できる。

$$\begin{aligned} & m \cdot e(g_1 g_2, g)^r / e(g_1 g_2, C_{2X})^{\frac{1}{x_i}} \\ &= m \cdot e(g_1 g_2, g)^r / e(g_1 g_2, g^{x_i r})^{\frac{1}{x_i}} = m \cdot e(g_1 g_2, g)^r / e(g_1 g_2, g)^r = m. \end{aligned}$$

[0160] [変形例 2]

変形例 1 の他に、以下に説明するように、再暗号化せずに暗号文データを復号する形態に変更しても良い。この場合も、鍵セットアップ処理、暗号化処理、復号処理のみを行えば良い。本変形例における鍵セットアップ処理、復号処理は、第 1 の実施形態における鍵セットアップ処理、復号処理とそれぞれ同じである。以下、本変形例における暗号化処理及び復号処理について説明する。なお、本変形例においては、復号装置 50 の識別情報を j とする。

[0161] 暗号化装置 20 の暗号化パラメータ生成部 23 は、ステップ ST 21 と同様に (s, s_k, s_v, k) を生成し (ST 21')、暗号化データ C_1 に検証鍵 s_v, k をセットする ($C_1 = s_v, k$)。

[0162] また、暗号化パラメータ生成部 23 は、5 つの乱数 $r, s, t, k, \theta \in \mathbb{Z}_p^*$ を生成して暗号文生成部 24 に送出する。

[0163] 暗号文生成部 24 は、これらの乱数 r, s, t, k, θ 及び復号装置 50 の公開鍵 p, k_j を用いて、平文データとしてのメッセージ $m \in G_T$ に対して、以下の暗号化データ $C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{221}', C_{221}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4$ を生成する (ST 22')。

[数14]

$$\begin{aligned} C_{2X}' &= Y_{2j}^s, C_{2X}'' = Y_{2j}^{rs}, C_{2Y}' = X_j^t, C_{2Y}'' = X_j^{rt}, \\ C_{2Z}' &= Y_{2j}^k, C_{2Z}'' = Y_{2j}^{rk}, C_{2Z1}' = X_j^k, C_{2Z1}'' = X_j^{rk}, \\ C_3 &= e(g_1 g_2, g)^r \cdot m, C_4 = (u^{sk} \cdot v)^r, \\ C_{5X} &= (g_1 \cdot g^\theta)^{\frac{1}{s}}, C_{5Y} = g^{\frac{\theta+1}{t}}, C_{5Z} = (g_1 \cdot g^{\theta+1})^{\frac{1}{k}} \end{aligned}$$

[0164] ステップ ST 22' の終了後、暗号文生成部 24 は、ステップ ST 23 と同様に、使い捨て署名 σ を生成する。

[0165] しかる後、暗号文生成部 24 は、上記全ての暗号化データ $C_1 \sim C_4$ と使い捨て署名 σ とを含む暗号文データ $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{221}', C_{221}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部 21 に書き込む。

[0166] 通信部 22 は、制御部 25 に制御されて一時データ記憶部 21 内の暗号文

データ C_j を復号装置 50 に送信する。

[0167] 復号装置 50 は、暗号化装置 20 において生成された暗号文データ C_j をステップ S T 51 と同様に検証する。検証が成功した場合、復号装置 50 は、秘密鍵 $s k_j$ を用いて、次式のように暗号文データ C_j を復号し、メッセージ m を得る。

[数15]

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

上式の復号結果が m となることは、次式により確認できる。なお、次式では、

$g_1 = g^\alpha$, $g_2 = g^\beta$ と書き替えて表記している。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{(1+\alpha+\theta)/k}, g^{\beta y_j r k})}{e(g^{(\alpha+\theta)/s}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(1+\alpha+\theta)/k}, g^{x_j r k})}{e(g^{(\theta+1)/t}, g^{x_j r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{1+\alpha+\theta}, g^{\beta r})}{e(g^{\alpha+\theta}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{1+\alpha+\theta}, g^r)}{e(g^{\theta+1}, g^r)} \right) \right\} \\ &= m \cdot e(g_1 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\alpha r}) = m. \end{aligned}$$

[0168] [変形例 3]

第 1 の実施形態では、公開パラメータにシステム固定値の 3 つの元 g , g_1 , g_2 が含まれる例を説明したが、これに限らず、元 g_2 を生成せず、公開パラメータに元 g_2 を含めなくてもよい。この場合、第 1 の実施形態において、 $g_2 = g$ として、 g_2 を g に置き換えればよい。これは後述する実施形態や変形例においても同様である。[

[変形例 4]

第 1 の実施形態では、公開パラメータにシステム固定値の 3 つの元 g , g_1 , g_2 が含まれる例を説明したが、これに限らず、システム固定値の 4 つ以上の元を含めてもよい。例えば、公開パラメータに 4 つの元 g , g_1 , g_2 , g_3 を含める場合、第 1 の実施形態において、 $g_2 = g_2 g_3$ として、 g_2 を $g_2 g_3$ に置き

換えればよい。また、例えば、公開パラメータに5つの元 g, g^1, g^2, g^3, g^4 を含める場合、第1の実施形態において、 $g^1 = g^{1 \cdot g^3}, g^2 = g^{2 \cdot g^4}$ として、 g^1 を $g^{1 \cdot g^3}$ に、 g^2 を $g^{2 \cdot g^4}$ にそれぞれ置き換えればよい。これは後述する実施形態や変形例においても同様である。

[0169] (第2の実施形態)

本実施形態では、再暗号化鍵をある期間毎に更新する例を説明する。期間を表すパラメータとして、時間パラメータ L を用いる。鍵セット T の処理、暗号化処理、再暗号化鍵生成処理、及び復号処理の内、暗号化処理、再暗号化鍵生成処理、及び再暗号化処理において時間パラメータ L が用いられる。例えば、ある期間 t_1 において暗号化処理を行う場合、 $L = t_1$ として後述する暗号化処理を行い、次の期間 t_2 において暗号化処理を行う場合、 $L = t_2$ として後述する暗号化処理を行う、というように時間パラメータを用いる。以下、本実施形態における鍵セット T の処理、暗号化処理、再暗号化鍵生成処理、再暗号化処理、及び復号処理について説明する。なお、上述の第1の実施の形態と共通する部分については、同一の符号を使用して説明したり、説明を省略したりする。

[0170] (1) 鍵セット T の処理

公開パラメータは、第1の実施形態と同じである。公開鍵・秘密鍵生成部14は、再暗号化鍵生成装置30の識別情報を！としたとき、再暗号化鍵生成装置30の秘密鍵 $x_i, y_i, z_i, w_i \in Z_p^*$ を生成し、この秘密鍵 $s_k = (x_i, y_i, z_i, w_i)$ を用いて再暗号化鍵生成装置30の公開鍵[数16]

$$pk_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i}, W_i, W_{1i})$$

を生成する(ST7)。ここで、

$$X_i = g^{x_i}, Y_{1i} = g^{y_i}, Y_{2i} = g^{y_i}, Z_i = g^{z_i}, Z_{1i} = g^{z_i}, W_i = g^{w_i}, W_{1i} = g^{w_i}$$

[0171] である。

[0172] また同様に、公開鍵・秘密鍵生成部14は、復号装置50の識別情報を！

としたとき、復号装置50の秘密鍵 $s_k = (x_j, y_j, z_j, w_j)$ を生成し

、この秘密鍵 s_k を用いて復号装置 50 の公開鍵

[数17]

$$pk_j = (X_j, Y_j, X_{2j}, Y_{2j}, Z_j, W_j, W_{1j})$$

を生成する (ST10)。ここで、

$$X_j = g^{x_j}, Y_j = g^{y_j}, X_{2j} = g^{x_{2j}}, Y_{2j} = g^{y_{2j}}, Z_j = g^{z_j}, Z_{1j} = g^{z_{1j}}, W_j = g^{w_j}, W_{1j} = g^{w_{1j}}$$

[0173] である。

[0174] (2) 暗号化処理

第1の実施形態と同様に、暗号化装置20の暗号化パラメータ生成部23

は、 (s_k, s_vk) を生成し (ST21)、暗号化データ C_1 に検証鍵 s

v_k をセットする ($C_1 = s \vee k$)。

[0175] また、暗号化パラメータ生成部23は、乱数 $r \in \mathbb{Z}_p^*$ を生成して暗号文生成

部24に送出する。

[0176] 暗号文生成部24は、この乱数 r 、再暗号化鍵生成装置30の公開鍵 pk_1

、及び時間パラメータ L を用いて、平文データとしてのメッセージ $m \in G_1$ に

対して、以下の暗号化データ $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4$ を生成する

(ST22)。

[数18]

$$\begin{aligned} C_{2X} &= X_1^r, C_{2Y} = Y_1^r, C_{2Z} = Z_1^r, C_{2Z1} = Z_{11}^r, \\ C_{2F} &= F_1(L)^r, C_3 = e(g_1 g_2, g)^r \cdot m, C_4 = (u^{sk} \cdot v)^r \end{aligned}$$

ここで、関数 $F_1(L)$ は次式により定義される。

$$F_1(L) = g^L \cdot W_1 = g^{L+w_1} \quad (L \in \mathbb{Z})$$

ステップ22の終了後、暗号文生成部24は、時間パラメータ L 及び暗号化データ

C_3, C_4 に対し、公開パラメータにおける署名生成機能 $\hat{s}$ とステップ21で生成し

た署名鍵 s_k による使い捨て署名 σ を次式に示すように生成する (ST23)。

$$\sigma = \hat{s}(s_k, (L, C_3, C_4))$$

[0177] しかる後、暗号文生成部24は、時間パラメータ L 、上記全ての暗号化データ $C_1 \sim C_4$ 、及び使い捨て署名 σ を含む暗号文データ $C_1 = (L, C_1, C_{2X},$

$C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, \sigma$) を生成し、得られた暗号文データを一時データ記憶部 21 に書き込む。

[0178] (3) 再暗号化鍵生成処理

乱数生成部 36 は、3つの乱数 $\theta, \delta_x, \delta_y \in Z_p^*$ を生成して再暗号化鍵生成部 34 に送出する。

[0179] 再暗号化鍵生成部 34 は、これらの乱数 $\theta, \delta_x, \delta_y$ 、秘密鍵記憶部 31 内の再暗号化鍵生成装置 30 の秘密鍵 s_{k_i} 、一時データ記憶部 32 内の復号装置 50 の公開鍵 p_{k_j} 、及び時間パラメータ L を用いて、再暗号化鍵 R_{ijL} を次式に示すように生成する (ST32)。

[数19]

$$R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$$

ここで、

$$\begin{aligned} R_{ijL1} &= (X_j \cdot g^\theta)^{1/x_i} \cdot F_i(L)^{\delta_x} = g^{\frac{x_j + \theta}{x_i} + (L + w_i)\delta_x}, \\ R_{ijL2} &= (Y_{2j} \cdot g^\theta)^{1/y_i} \cdot F_i(L)^{\delta_y} = g^{\frac{\beta y_j + \theta}{y_i} + (L + w_i)\delta_y}, \\ R_{ijL3} &= (X_j \cdot Y_{2j} \cdot g^\theta)^{1/z_i} = g^{\frac{x_j + \beta y_j + \theta}{z_i}}, \\ R_{ijL4} &= X_i^{\delta_x} = g^{x_i \delta_x}, R_{ijL5} = Y_{1i}^{\delta_y} = g^{\alpha y_i \delta_y} \end{aligned}$$

[0180] である。なお、上式では、 $g_1 = g^\alpha$ 、 $g_2 = g^\beta$ と書き替えて表記している。

[0181] (4) 再暗号化処理

再暗号化処理部 44 は、公開パラメータ、時間パラメータ L 、及び次の検証式を用い、一時データ記憶部 42 内の暗号文データ C_i を検証する (ST41)。

[数20]

$$\begin{aligned}
e(C_{2X}, u^{C_1} \cdot v) &= e(X_i, C_4) \\
e(C_{2Y}, u^{C_1} \cdot v) &= e(Y_{1i}, C_4) \\
e(C_{2Z}, u^{C_1} \cdot v) &= e(Z_i, C_4) \\
e(C_{2Z1}, u^{C_1} \cdot v) &= e(Z_{1i}, C_4) \\
e(C_{2F}, u^{C_1} \cdot v) &= e(F_i(L), C_4) \\
V(C_1, \sigma, (L, C_3, C_4)) &= 1
\end{aligned}$$

[0182] ここで、上記6つの検証式が全て成立すれば検証は成功し、1つでも成立しない検証式があれば検証は失敗する。

[0183] 検証が成功した場合、再暗号化パラメータ生成部45は、4つの乱数 $s, t, k, h \in Z_p^*$ を生成して再暗号化処理部44に送出する。

[0184] 再暗号化処理部44は、これらの乱数 s, t, k, h 、一時データ記憶部42内の暗号文データ C_i 、一時データ記憶部42内の再暗号化鍵 R_{ijL} 、及び時間パラメータ L を用いて、次式に示すように、再暗号化データ C_{2X}' , C_{2X}'' , C_{2Y}' , C_{2Y}'' , C_{2Z}' , C_{2Z}'' , C_{2Z1}' , C_{2Z1}'' , C_{2F}' , C_{2F}'' , C_{5X} , C_{5Y} , C_{5Z} , C_{5FX} , C_{5FY} を生成する (ST42)。

[数21]

$$\begin{aligned}
C_{2X}' &= X_i^s, C_{2X}'' = C_{2X}^s = X_i^{rs}, C_{2Y}' = Y_{1i}^t, C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, \\
C_{2Z}' &= Z_i^k, C_{2Z}'' = C_{2Z}^k = Z_i^{rk}, C_{2Z1}' = Z_{1i}^k, C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk}, \\
C_{2F}' &= F_i(L)^h, C_{2F}'' = C_{2F}^h = F_i(L)^{rh},
\end{aligned}$$

$$C_{5X} = R_{iL1}^{\frac{1}{s}}, C_{5Y} = R_{iL2}^{\frac{1}{t}}, C_{5Z} = R_{iL3}^{\frac{1}{k}}, C_{5FX} = R_{iL4}^{\frac{1}{h}}, C_{5FY} = R_{iL5}^{\frac{1}{h}}$$

[0185] ステップST42の終了後、再暗号化処理部44は、時間パラメータ L 、上記全ての暗号化データ再暗号化データ $C_{2X}' \sim C_{5FY}$ を、暗号文データ C_i 内の暗号化データ C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} と置換して再暗号文データ $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部42に書き込む。

[0186] (5) 復号処理

復号処理部 54 は、公開パラメータ及び自装置 50 の公開鍵 $p k_j$ と次の検証式を用い、一時データ記憶部 52 内の再暗号文データ C_j を検証する (S T 51)。

[数22]

$$\begin{aligned}
 e(C_{2X}'', u^{C_1} \cdot v) &= e(C_{2X}', C_4) \\
 e(C_{2Y}'', u^{C_1} \cdot v) &= e(C_{2Y}', C_4) \\
 e(C_{2Z}'', u^{C_1} \cdot v) &= e(C_{2Z}', C_4) \\
 e(C_{2Z1}'', u^{C_1} \cdot v) &= e(C_{2Z1}', C_4) \\
 e(C_{2F}'', u^{C_1} \cdot v) &= e(C_{2F}', C_4) \\
 e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') &= e(C_{5X}, C_{2X}') \cdot e(Y_{2j}, g) \\
 e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') &= e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_1) \\
 \mathcal{V}(C_1, \sigma, (L, C_3, C_4)) &= 1
 \end{aligned}$$

[0187] ここで、上記 8 つの検証式が全て成立すれば検証は成功し、1 つでも成立しない検証式があれば検証は失敗する。

[0188] 検証が成功した場合、復号処理部 54 は、自装置の秘密鍵 $s k_j$ を用いて、次式に示すように、再暗号文データ C_j を復号し、メッセージ m を得る (S T 52)。

[数23]

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}$$

上式の復号結果が m となることは、次式により確認できる。なお、次式では、 $g_1 = g^\alpha$ 、 $g_2 = g^\beta$ と書き替えて表記している。

$$\begin{aligned}
 & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\
 &= C_3 / \left\{ \left(\frac{e(g^{\frac{x_j + \beta y_j + \theta}{z_i k}}, g^{z_i r k}) \cdot e(g^{\frac{x_j \delta_z}{k}}, g^{(L + w_i) r h})}{e(g^{\frac{((x_j + \theta)/x_i) + (L + w_i) \delta_z}{s}}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{x_j + \beta y_j + \theta}{z_i k}}, g^{\alpha x_i r k}) \cdot e(g^{\frac{\alpha y_j \delta_y}{h}}, g^{(L + w_i) r h})}{e(g^{\frac{((\beta y_j + \theta)/y_i) + (L + w_i) \delta_y}{t}}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\} \\
 &= C_3 / \left\{ \left(\frac{e(g^{x_j + \beta y_j + \theta}, g^r) \cdot e(g^{x_i \delta_z}, g^{(L + w_i) r})}{e(g^{(x_j + \theta) + (L + w_i) x_i \delta_z}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{x_j + \beta y_j + \theta}, g^{\alpha r}) \cdot e(g^{\alpha y_i \delta_y}, g^{(L + w_i) r})}{e(g^{(\beta y_j + \theta) + (L + w_i) y_i \delta_y}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\
 &= m \cdot e(g_1 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\alpha r}) = m.
 \end{aligned}$$

[0189] なお、本実施形態は、適宜、処理の順番を変更してもよい。例えば、復号処理と暗号文検証処理の順番を変更してもよい。同様に、再暗号化鍵生成処理の順番を暗号化処理よりも前に変更してもよい。

[0190] 上述したように本実施形態によれば、再暗号化鍵 R_{ijL} を乱数 θ , δ_x , δ_y 及び時間パラメータ L に基づいて生成する構成により、第1の実施形態の効果に加え、復号権限を移譲するか否かを期間毎に決めることができ、よりきめ細かいアクセス制御が可能となる。また、これにより、ある期間においてユーザA向けの暗号文についての復号権限を一度ユーザBへ移譲した後でも、次の期間についてはユーザA向けの暗号文についての復号権限をユーザBに与えない、つまり、（ユーザA向けの暗号文についての）ユーザBの復号権限を無効化することが可能となるため、利便性がより向上したファイル共有システムを提供することができる。

[0191] [変形例5]

第2の実施形態では、暗号化装置20において暗号文データを生成し、再暗号化装置40において暗号文データを再暗号化して再暗号文データを生成し、復号装置50において再暗号文データを復号する例を挙げたが、再暗号化せずに暗号文データを復号する形態に変更しても良い。この場合、鍵セットアップ処理、暗号化処理、復号処理のみを行えば良い。本変形例における鍵セットアップ処理は、第2の実施形態における鍵セットアップ処理と同じである。以下、本変形例における暗号化処理及び復号処理について説明する。

[0192] 本変形例における暗号化処理と、第2の実施形態における暗号化処理との違いは、最終ステップのみである。前述の記号を流用して説明をするために、便宜上、復号装置50の識別情報を i とする。この場合、暗号化装置20の通信部22は、制御部25に制御されて一時データ記憶部21内の暗号文データ C_i を復号装置50に送信する（ST24'）。

[0193] 復号装置50は、暗号化装置20において生成された暗号文データ C_i をステップST41と同様に検証する。検証が成功した場合、復号装置50は、

秘密鍵 $s k_i$ を用いて、次式のように暗号文データ C_i を復号し、メッセージ m を得る。

[数24]

$$m = C_3 / e(g_1 g_2, C_{2X})^{\frac{1}{z_i}}$$

上式の復号結果が m となることは、次式により確認できる。

$$\begin{aligned} m \cdot e(g_1 g_2, g)^r / e(g_1 g_2, C_{2X})^{\frac{1}{z_i}} \\ = m \cdot e(g_1 g_2, g)^r / e(g_1 g_2, g^{x_i r})^{\frac{1}{z_i}} = m \cdot e(g_1 g_2, g)^r / e(g_1 g_2, g)^r = m. \end{aligned}$$

[0194] [変形例 6]

変形例 5 の他に、以下に説明するように、再暗号化せずに暗号文データを復号する形態に変更しても良い。この場合も、鍵セットアップ処理、暗号化処理、復号処理のみを行えば良い。本変形例における鍵セットアップ処理、復号処理は、第 2 の実施形態における鍵セットアップ処理、復号処理とそれぞれ同じである。以下、本変形例における暗号化処理及び復号処理について説明する。なお、本変形例においては、復号装置 50 の識別情報を j とする。

[0195] 暗号化装置 20 の暗号化パラメータ生成部 23 は、ステップ ST 21 と同様に $(s s k, s v k)$ を生成し (ST 21')、暗号化データ C_1 に検証鍵 $s v k$ をセットする ($C_1 = s v k$)。

[0196] また、暗号化パラメータ生成部 23 は、8 つの乱数 $r, s, t, k, h, \theta, \delta_x, \delta_y \in Z_p^*$ を生成して暗号文生成部 24 に送出する。

[0197] 暗号文生成部 24 は、これらの乱数 $r, s, t, k, h, \theta, \delta_x, \delta_y$ 、復号装置 50 の公開鍵 $p k_j$ 、及び時間パラメータ L を用いて、平文データとしてのメッセージ $m \in G_T$ に対して、以下の暗号化データ $C_{2X}', C_{2X}''', C_{2Y}', C_{2Y}''', C_{2Z}', C_{2Z}''', C_{2Z1}', C_{2Z1}''', C_{2F}', C_{2F}''', C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3, C_4$ を生成する (ST 22')。

[数25]

$$\begin{aligned}
C'_{2X} &= Y_{2j}^s, C''_{2X} = Y_{2j}^{rs}, C'_{2Y} = X_j^t, C''_{2Y} = X_j^{rt}, \\
C'_{2Z} &= Y_{2j}^k, C''_{2Z} = Y_{2j}^{rk}, C'_{2Z1} = X_j^k, C''_{2Z1} = X_j^{rk}, \\
C'_{2F} &= F_i(L)^h, C''_{2F} = F_i(L)^{rh}, \\
C_3 &= e(g_1 g_2, g)^r \cdot m, C_4 = (u^{sk} \cdot v)^r, \\
C_{5X} &= (g_1 \cdot g^\theta \cdot F_j(L)^{\delta_y})^{\frac{1}{s}} = g^{\frac{\alpha + \theta + (L + w_j)\delta_y}{s}}, \\
C_{5Y} &= (g^{1+\theta} \cdot F_j(L)^{\delta_x})^{\frac{1}{t}} = g^{\frac{1 + \theta + (L + w_j)\delta_x}{t}}, \\
C_{5Z} &= (g_1 \cdot g^{1+\theta})^{\frac{1}{k}} = g^{\frac{\alpha + 1 + \theta}{k}}, \\
C_{5FX} &= (Y_{2j})^{\frac{\delta_y}{h}}, C_{5FY} = (X_j)^{\frac{\delta_x}{h}}
\end{aligned}$$

[0198] ステップST22'の終了後、暗号文生成部24は、ステップST23と同様に、使い捨て署名 σ を生成する。

[0199] しかる後、暗号文生成部24は、時間パラメータL、上記全ての暗号化データ $C_1 \sim C_4$ と使い捨て署名 σ とを含む暗号文データ $C_j = (L, C'_{2X}, C''_{2X}, C'_{2Y}, C''_{2Y}, C'_{2Z}, C''_{2Z}, C'_{2Z1}, C''_{2Z1}, C'_{2F}, C''_{2F}, C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部21に書き込む。

[0200] 通信部22は、制御部25に制御されて一時データ記憶部21内の暗号文データ C_j を復号装置50に送信する。

[0201] 復号装置50は、暗号化装置20において生成された暗号文データ C_j をステップST51と同様に検証する。検証が成功した場合、復号装置50は、秘密鍵 $s k_j$ を用いて、次式のように暗号文データ C_j を復号し、メッセージ m を得る。

[数26]

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{z_j}} \right\}$$

上式の復号結果がmとなることは、次式により確認できる。なお、次式では、

$g_1 = g^\alpha$, $g_2 = g^\beta$ と書き替えて表記している。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{z_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\frac{\alpha+1+\theta}{k}}, g^{\beta y_j r k}) \cdot e(g^{\frac{\beta y_j \delta y}{k}}, g^{(L+w_j) r h})}{e(g^{\frac{\alpha+\theta+(L+w_j)\delta y}{k}}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\alpha+1+\theta}{k}}, g^{x_j r k}) \cdot e(g^{\frac{x_j \delta x}{k}}, g^{(L+w_j) r h})}{e(g^{\frac{1+\theta+(L+w_j)\delta x}{k}}, g^{x_j r t})} \right)^{\frac{1}{z_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\alpha+1+\theta}, g^{\beta r}) \cdot e(g^{\beta \delta y}, g^{(L+w_j) r})}{e(g^{\alpha+\theta+(L+w_j)\delta y}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{\alpha+1+\theta}, g^r) \cdot e(g^{\delta x}, g^{(L+w_j) r})}{e(g^{1+\theta+(L+w_j)\delta x}, g^r)} \right) \right\} \\ &= m \cdot e(g_1 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\alpha r}) = m. \end{aligned}$$

[0202] 以上説明した少なくとも一つの実施形態によれば、再暗号化鍵を乱数に基づいて生成する構成により、サーバとユーザが結託した場合でも、復号権限が移譲元の許可なく再移譲されることを阻止することができる。

[0203] なお、上記の各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0204] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

[0205] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0206] さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に

限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

[0207] また、記憶媒体は1つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0208] なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

[0209] また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0210] なお、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

[請求項1] 第1 ユーザ装置の第1 公開鍵により平文データを暗号化して得られた暗号文データを復号せずに再暗号化して、第2 ユーザ装置の第2 秘密鍵により復号可能な再暗号文データを取得するための再暗号化鍵を生成する再暗号化鍵生成装置（30）であって、

前記第1 公開鍵に対応する第1 秘密鍵を記憶する第1 記憶手段（31）と、

前記第2 秘密鍵に対応する第2 公開鍵を記憶する第2 記憶手段（32）と、

第1 乱数を生成する第1 乱数生成手段（36）と、

前記第1 秘密鍵、前記第2 公開鍵及び前記第1 乱数に基づいて、前記再暗号化鍵を生成する再暗号化鍵生成手段（34）と

を備えたことを特徴とする再暗号化鍵生成装置。

[請求項2] 請求項1 に記載の再暗号化鍵生成装置において、

再暗号化鍵生成手段（34）は、再暗号化前の暗号文データには依存せずに、前記第1 秘密鍵、前記第2 公開鍵及び前記第1 乱数に基づいて、前記再暗号化鍵を生成することを特徴とする再暗号化鍵生成装置。

[請求項3] 請求項1 に記載の再暗号化鍵生成装置において、

前記第1 公開鍵は、前記第1 秘密鍵及び複数のシステム固定値に基づいて生成されており、

前記第2 公開鍵は、前記第2 秘密鍵及び前記複数のシステム固定値に基づいて生成されていることを特徴とする再暗号化鍵生成装置。

[請求項4] 請求項2 に記載の再暗号化鍵生成装置において、

前記第1 秘密鍵を $sk_1 = (x_1, y_1, z_1)$ で表し、前記第2 秘密鍵を $sk_2 = (x_2, y_2, z_2)$ で表し、前記第1 乱数を θ で表し、前記複数のシステム固定値を g, g_1, g_2 で表し（但し、双線型写像 $e : G \times G \rightarrow G_T$ が存在する素数位数 p の群である双線型写像群

を G , G_T で表したとき、 $g, g_1, g_2 \in G$ ）、前記各システム固定値に関するベキ指数を β で表し（但し、 $g_2 = g^\beta$ ）、前記再暗号化鍵を R_{ij} で表すとき、

[数1]

$$R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$$

であり（但し、

$$R_{ij1} = g^{\frac{x_j + \theta}{x_i}}, R_{ij2} = g^{\frac{\beta y_j + \theta}{y_i}}, R_{ij3} = g^{\frac{x_j + \beta y_j + \theta}{z_i}}$$

）、

前記第1公開鍵を pk_i で表すとき、

$$pk_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i})$$

であり（但し、

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Y_{2i} = g_2^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}$$

）、

前記第2公開鍵を pk_j で表すとき、

$$pk_j = (X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j})$$

であり（但し、

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Y_{2j} = g_2^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}$$

）、

前記平文データを m で表し（但し、 $m \in G_T$ ）、第2乱数を r で表し、前記暗号文データを C_i で表すとき（但し、前記双線型写像 $e : G \times G \rightarrow G_T$ を $e(,)$ で表す）、

$$C_i = (C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)$$

であり（但し、

[数2]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, C_3 = e(g_1 g_2, g)^r \cdot m$$

)、

前記再暗号文データを C_j で表すとき（但し、第3乃至第5乱数を s, t, k で表す）、

$$C_j = (C_{2X}^{'}, C_{2Y}^{'}, C_{2Z}^{'}, C_{2Z1}^{'}, C_{5X}, C_{5Y}, C_{5Z}, C_3)$$

であり（但し、

[数3]

$$C_{2X}'' = C_{2X}^s = X_i^{rs}, \quad C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, \quad C_{2Z}'' = C_{2Z}^k = Z_i^{rk}, \quad C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk}, \\ C_{5X} = R_{ij1}^{\frac{1}{s}}, \quad C_{5Y} = R_{ij2}^{\frac{1}{t}}, \quad C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

)、

前記平文データ m 、前記再暗号文データ C_j 及び前記第2秘密鍵 s_k_j の関係は、

$$m = C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{s_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{t_j}} \right\}$$

で表されることを特徴とする再暗号化鍵生成装置。

[請求項5]

第1ユーザ装置の第1公開鍵により平文データを暗号化して得られた暗号文データを復号せずに再暗号化して、第2ユーザ装置の第2秘密鍵により復号可能な再暗号文データを取得するための再暗号化鍵を生成する再暗号化鍵生成装置（30）に通信可能な再暗号化装置（40）であって、

前記再暗号化鍵生成装置から受けた前記再暗号化鍵を記憶する記憶手段（41）と、

前記第1ユーザ装置から受けた前記暗号文データを復号せずに、前記記憶手段内の再暗号化鍵により再暗号化して前記再暗号文データを取得する再暗号化手段（44）と、

前記得られた再暗号文データを前記第2ユーザ装置に送信する手段（43）と、

を備え、

前記再暗号化鍵は、前記第1公開鍵に対応する第1秘密鍵、前記第2秘密鍵に対応する第2公開鍵、及び前記再暗号化鍵生成装置により

生成された第1乱数に基づいて、生成されていることを特徴とする再暗号化装置。

[請求項6]

請求項5に記載の再暗号化装置において、
前記再暗号化鍵は、再暗号化前の暗号文データには依存せずに生成されていることを特徴とする再暗号化装置。

[請求項7]

第1ユーザ装置の第1公開鍵により平文データを暗号化して得られた暗号文データを復号せずに再暗号化して、第2ユーザ装置の第2秘密鍵により復号可能な再暗号文データを取得するための再暗号化鍵を生成する再暗号化鍵生成装置(30)のプロセッサに実行され、非一時的なコンピュータ読取可能な記憶媒体(M3)に記憶されたプログラムであって、

前記第1公開鍵に対応する第1秘密鍵を前記再暗号化鍵生成装置の第1記憶手段(31)に書込む処理を前記プロセッサに実行させる第1プログラムコード(33)、

前記第2秘密鍵に対応する第2公開鍵を前記再暗号化鍵生成装置の第2記憶手段(32)に書込む処理を前記プロセッサに実行させる第2プログラムコード(ST31)、

第1乱数を生成する処理を前記プロセッサに実行させる第3プログラムコード(36)、

前記第1秘密鍵、前記第2公開鍵及び前記第1乱数に基づいて、前記再暗号化鍵を生成する処理を前記プロセッサに実行させる第4プログラムコード(32)、

を備えたプログラム。

[請求項8]

請求項7に記載のプログラムにおいて、
前記再暗号化鍵を生成する処理は、再暗号化前の暗号文データには依存せずに前記プロセッサに実行させることを特徴とするプログラム。
。

[請求項9]

第1ユーザ装置の第1公開鍵により平文データを暗号化して得られ

暗号文データを復号せずに再暗号化して、第２ユーザ装置の第２秘密鍵により復号可能な再暗号文データを生成するための再暗号化鍵を生成する再暗号化鍵生成装置（４０）に通信可能な再暗号化装置（４０）のプログラムを実行させ、非一時的なコンピュータ読取可能な記憶媒体（Ｍ４）に記憶されたプログラムであって、

前記再暗号化鍵生成装置から受けた前記再暗号化鍵を前記再暗号化装置の記憶手段（４１）に書き込む処理を前記プログラムを実行させる

第１プログラムコード（４３）、

前記第１ユーザ装置から受けた前記暗号文データを復号せずに、前記記憶手段内の再暗号化鍵により再暗号化して前記再暗号文データを再暗号化処理を前記プログラム（４４）に実行させる第２プログラムコード（４４）に実行させ、非一時的なコンピュータ読取可能な記憶媒体（Ｍ２）に記憶されたプログラムであって、

前記第１公開鍵を前記暗号化装置の記憶手段（２１）に書き込む処理を前記プログラム（２２）に実行させる第１プログラムコード（２２）、

前記記憶手段内の第１公開鍵を用いて前記平文データを暗号化して前記暗号文データを再暗号化処理を前記プログラム（２２）に実行させる第２プログラムコード（２２）

[請求項10]

グラムコード（S T 2 2）、

前記得られた暗号文データを前記再暗号化装置に送信する処理を前記プロセッサに実行させる第3プログラムコード（S T 2 4）、

を備え、

前記再暗号化鍵は、前記第1公開鍵に対応する第1秘密鍵、前記第2秘密鍵に対応する第2公開鍵、及び当該再暗号化鍵を生成する再暗号化鍵生成装置（30）により生成された第1乱数に基づいて、生成されているプログラム。

[請求項11]

再暗号化装置が再暗号化鍵に基づいて、第1ユーザ装置の第1公開鍵により平文データを暗号化して得られた暗号文データを復号せずに再暗号化して、第2ユーザ装置の第2秘密鍵により復号可能な再暗号文データを得た後に、前記再暗号化装置（40）から受けた前記再暗号文データを復号する復号装置（50）のプロセッサに実行され、非一時的なコンピュータ読取可能な記憶媒体（M5）に記憶されたプログラムであって、

前記第2秘密鍵を前記復号装置の記憶手段（51）に書込む処理を前記プロセッサに実行させる第1プログラムコード（53）、

前記再暗号化装置から前記再暗号文データを受けると、前記記憶手段内の第2秘密鍵に基づいて、当該再暗号文データを復号して前記平文データを得る処理を前記プロセッサに実行させる第2プログラムコード（54）、

を備え、

前記再暗号化鍵は、前記第1公開鍵に対応する第1秘密鍵、前記第2秘密鍵に対応する第2公開鍵、及び当該再暗号化鍵を生成する再暗号化鍵生成装置（30）により生成された第1乱数に基づいて、生成されているプログラム。

[請求項12]

請求項9乃至請求項11のいずれか1項に記載のプログラムにおいて、

前記再暗号化鍵は、再暗号化前の暗号文データには依存せずに生成されることを特徴とするプログラム。