

明 細 書

発明の名称：

再暗号化鍵生成装置、再暗号化装置、暗号化装置、復号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、暗号化装置、復号装置及びプログラムに関する。

背景技術

[0002] 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ため再暗号化する方法がある。

先行技術文献

非特許文献

[0003] 非特許文献1：R. Hayashi, T. Matsushita, T. Yoshida, Y. Fujii, and K. Okada, "Unforgeability of Re-Encryption Keys against Collusion Attack in Proxy Re-Encryption," In Proc. IWSEC 2011, LNCS 7038, pp. 210-229, Springer-Verlag, 2011.

発明の概要

発明が解決しようとする課題

[0004] 従来の再暗号化方式は、特に問題は無いが、しいて言えば、サーバが各ユーザの許可なしに再暗号文を作成可能な状態にある。このため、プロキシ再暗号化方式は、安全なファイル共有を実現する観点から、改善の余地がある。

課題を解決するための手段

[0005] 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得るための再暗号化鍵を生成する。

[0006] 前記再暗号化鍵生成装置は、第1記憶手段、第2記憶手段及び再暗号化鍵生成手段を備えている。

[0007] 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。

[0008] 前記第2記憶手段は、前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵を記憶する。

[0009] 前記再暗号化鍵生成手段は、前記第1秘密鍵及び前記第2再暗号化鍵生成鍵に基づいて、前記再暗号化鍵を生成する。

図面の簡単な説明

[0010] [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。

[図9]図9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10]図10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11]図 1 1 は、同実施形態に係る再暗号化鍵生成装置の構成を示す模式図である。

[図12]図 1 2 は、第 1 3 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13]図 1 3 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14]図 1 4 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15]図 1 5 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16]図 1 6 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17]図 1 7 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18]図 1 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

[0011] 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 又は図 1 2 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 から各コンピュータにインストールされ、当該各コンピュータのプロセッサに実行されることにより、各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。

[0012] (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。

[0013] (鍵生成) $\text{KeyGen}(\lambda) \rightarrow (pk, sk)$

鍵生成アルゴリズムKeyGenは、セキュリティパラメータ λ 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。

[0014] (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。

[0015] (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。

[0016] (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。

[0017] (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。

[0018] 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。

[0019] 例えば、本実施形態に示す再暗号化方式のように、暗号化、復号、再暗号化鍵生成、再暗号化の各関数の入力として公開パラメータ（詳しくは後述する）を含んでいても良い。

[0020] 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ReKeyGen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（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 $s k_A$ に代えて、ユーザB宛の再暗号化鍵 $r k_{A \rightarrow B}$ とユーザCの秘密鍵 $s k_C$ とが入力されるモデルなども考えられている。

[0021] 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。

[0022] 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。

[0023] また、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ReKeyGenにおいて、ユーザBの公開鍵 $p k_B$ に代えて、ユーザBの再暗号化鍵生成鍵 $r k_B$ を入力するようにしても良い。この場合、鍵生成アルゴリズムKeyGenと再暗号化鍵生成アルゴリズムReKeyGenは、以下のように表される。

[0024] (鍵生成) $\text{KeyGen}(\lambda) \rightarrow (p k, s k, r k, p a r)$

鍵生成アルゴリズムKeyGenは、セキュリティパラメータ λ が入力されると、公開鍵 $p k$ 、秘密鍵 $s k$ 、及び再暗号化鍵生成鍵 $r k$ の組 $(p k, s k, r k)$ と公開パラメータ $p a r$ を出力する。なお、本実施形態では、この処理を鍵セットアップ処理と呼ぶ。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。

[0025] (再暗号化鍵生成) $\text{ReKeyGen}(s k_A, r k_B, p a r) \rightarrow r k_{A \rightarrow B}$

再暗号化鍵生成アルゴリズムReKeyGenは、ユーザAの秘密鍵 $s k_A$ 、ユーザBの再暗号化鍵生成鍵 $r k_B$ 、公開パラメータ $p a r$ が入力されると、再暗号化鍵 $r k_{A \rightarrow B}$ を出力する。

[0026] また、本実施形態に示す再暗号化方式のように、再暗号化アルゴリズムReEncの入力として、ユーザAの公開鍵 $p k_A$ と公開パラメータ $p a r$ を追加して

も良い。この場合、再暗号化アルゴリズムReEncは、以下のように表される。

[0027] (再暗号化) $\text{ReEnc}(r k_{A \rightarrow B}, C_A, p k_A, p a r) \rightarrow C_B$

再暗号化アルゴリズムReEncは、再暗号化鍵 $r k_{A \rightarrow B}$ と、ユーザA宛の暗号文 C_A と、ユーザAの公開鍵 $p k_A$ と、公開パラメータ $p a r$ とが入力されると、ユーザB宛の暗号文 C_B を出力する。

[0028] 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、…（以下、ユーザA、B、C、…と略記する場合もある。また、第1ユーザ装置、第2ユーザ装置、…と呼ぶこともある。）とを備えている。サーバS_vと、ユーザ装置A、B、C、…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。サーバS_vは1台のみを設けてもよく、複数台を設けても良い。

[0029] 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。

[0030] 事前準備として、グループ管理者は秘密鍵 $s k_{Gr}$ を持っているものとする。また、グループ管理者の公開鍵 $p k_{Gr}$ はサーバS_vの公開鍵記憶部1に記憶されているとする。また、各ユーザiは、秘密鍵 $s k_i$ と再暗号化鍵生成鍵 $r k_i$ を持っているものとする。つまり、ユーザAは $s k_A$ と $r k_A$ 、ユーザBは $s k_B$ と $r k_B$ 、ユーザCは $s k_C$ と $r k_C$ をそれぞれ持っている。なお、サーバS_vと各ユーザiは、公開パラメータ $p a r$ と各ユーザiの公開鍵 $p k_i$ を取得可能であるが、ここでは説明を省略し、詳しくは後述する。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。

- [0031] 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。ここで、 $E(PK, M)$ とは、公開鍵 PK を用いて平文 M を暗号化した暗号文を表す。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。
- [0032] 今、ユーザAがファイルデータ m を共有を承諾したとする。ユーザAは、グループ管理者へユーザAの再暗号化鍵生成鍵 $r k_A$ を送信する。グループ管理者は、グループ管理者の秘密鍵 $s k_{Gr}$ とユーザAの再暗号化鍵生成鍵 $r k_A$ を用いて、グループ管理者宛の暗号文 $E(p k_{Gr}, m)$ をユーザA宛の暗号文 $E(p k_A, m)$ に再暗号化する再暗号化鍵 $r k_{Gr \rightarrow A}$ を生成する。グループ管理者は、生成した再暗号化鍵 $r k_{Gr \rightarrow A}$ をサーバ S_v へ送信する。サーバ S_v は、再暗号化鍵記憶部3においてこの再暗号化鍵 $r k_{Gr \rightarrow A}$ を保管する。
- [0033] 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 $r k_{Gr \rightarrow A}$ を用いて、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。
- [0034] 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。
- [0035] 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。
- [0036] 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。

[0037] 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。これにより、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 の厳重な管理が不要となり、サーバ S_v の管理コストの低減に繋がる。

[0038] プロキシ再暗号化方式では、移譲元（上述の例ではグループ管理者）宛の暗号文を移譲先（上述の例ではユーザ A ）宛の暗号文に再暗号化することにより、暗号文の復号権限が移譲先へ移譲される。ここで、プロキシ再暗号化方式では、再暗号化鍵生成アルゴリズム $ReKeyGen$ の入力に、（移譲先の秘密鍵は含まれず）移譲先の公開鍵が含まれる。このため、例えばユーザ i が、ユーザ A の公開鍵 $p k_A$ を用いて別のファイルデータ m' を暗号化してユーザ A 宛の暗号文 $E(p k_A, m')$ を生成できるようにするために、ユーザ A の公開鍵 $p k_A$ は（例えばシステムを立ち上げる際など）予め公開される。

[0039] 一方、ユーザ A が暗号文の復号権限のユーザ A への移譲を承諾していない場合でも、ユーザ A の公開鍵 $p k_A$ が既に公開されているため、グループ管理者は再暗号化鍵 $r k_{Gr \rightarrow A}$ を生成できてしまう。従って、ユーザ A の承諾なく再暗号化（つまり、暗号文の復号権限のユーザ A への移譲）を行われてしまう可能性がある。

[0040] それに対して、本ファイル共有システムにおいては、移譲先であるユーザ A がユーザ A の再暗号化鍵生成鍵 $r k_A$ をグループ管理者に送信しなければ、グループ管理者は再暗号化鍵 $r k_{Gr \rightarrow A}$ を生成できない。従って、移譲先の承諾なく再暗号化（つまり、暗号文の復号権限の当該移譲先への移譲）を行えないようにすることができる。

[0041] ユーザ B がファイル共有を行う際も上記と同様である。

[0042] 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、セキュリティパラメータに基づいて、再暗号化システムの公開パラメータ及び各装置 30、50 の公開鍵・秘密鍵のペアと再暗号化鍵生成鍵を生成する。ここで、再暗号化鍵生成鍵は、各装置 30、50 の秘密鍵に対応する公開鍵とは異なる鍵である。なお、「再暗号化鍵生成鍵」の用語は、例えば、「再暗号化鍵生成データ」又は「再暗号化鍵生成許可データ」等といった所望の名称に読み替えてもよい。

[0043] 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と公開パラメータを用いて平文データを暗号化し、得られた暗号文データを再暗号化装置 40 に送信する。

[0044] 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 の再暗号化鍵生成鍵とに基づいて再暗号化鍵を生成し、得られた再暗号化鍵を再暗号化装置 40 に送信する。なお、復号装置 50 の再暗号化生成鍵は、復号装置 50 の秘密鍵に対応する公開鍵とは異なる。また、本実施形態では、再暗号化鍵が、再暗号化鍵生成装置 30 の秘密鍵と復号装置 50 の再暗号化鍵生成鍵と公開パラメータと乱数とに基づいて生成される。但し、再暗号化鍵の生成の際に、乱数は必須ではなく、省略してもよい。例えば、第 5 又は第 12 の実施形態では、再暗号化鍵が乱数を用いずに生成される。

[0045] 再暗号化装置 40 は、再暗号化鍵生成装置 30 の公開鍵、公開パラメータ、及び再暗号化鍵生成装置 30 から受けた再暗号化鍵に基づいて、暗号化装置 20 から受けた暗号文データを検証処理すると共に、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し、得られた再暗号文データを復号装置 50 に送信する。但し、検証処理は必須ではなく、省略してもよい。

[0046] 復号装置 50 は、自装置 50 の秘密鍵と公開パラメータに基づいて、再暗号化装置 40 から受けた再暗号文データを検証処理すると共に、再暗号化装置 40 から受けた再暗号文データを復号処理して平文データを得る。但し、検証処理は必須ではなく、省略してもよい。なお、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 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。また、暗号化装置 20 は、暗号化装置 20 の公開鍵と公開パラメータ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 に送信しても良い。この場合、鍵生成装置 10 は、公開パラメータ及び各装置 20、50 の公開鍵・秘密鍵のペアと再暗号化鍵生成鍵を生成する。再暗号化鍵生成装置 30 は、暗号化装置 20 の秘密鍵と復号装置 50 の再暗号化鍵生成鍵と公開パラメータと乱数とを用いて再暗号化鍵を生成し、得られた再暗号化鍵を再暗号化装置 40 に送信する。

[0047] 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と再暗号化鍵生成鍵を生成する場合、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と再暗号化鍵生成鍵を生成する場合、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。

[0048] 各エンティティは、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 の一部又は全部を保持しても良

い。つまり、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、ユーザ管理者とグループ管理者が同一の場合もあるし、異なる場合もある。また、ユーザがユーザ管理者、グループ管理者又は両者を兼ねる場合も兼ねない場合もある。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、秘密鍵、及び再暗号化鍵生成鍵は、第1ユーザ装置の第1公開鍵、第1秘密鍵、及び第1再暗号化鍵生成鍵、第2ユーザ装置の第2公開鍵、第2秘密鍵、及び第2再暗号化鍵生成鍵、…と呼んでもよい。

[0049] また、例えば、図9、図10にそれぞれ示すように、各エンティティが各装置を保持しても良い。図9において、サーバS v 2は鍵生成装置10を保持し、公開パラメータ、ユーザAの公開鍵と秘密鍵の組と再暗号化鍵生成鍵、及びユーザBの公開鍵と秘密鍵の組と再暗号化鍵生成鍵を生成する。サーバS v 2は、公開パラメータ、ユーザAの公開鍵と秘密鍵の組と再暗号化鍵生成鍵をユーザAに渡し、公開パラメータ、ユーザBの公開鍵と秘密鍵の組と再暗号化鍵生成鍵をユーザBに渡し、公開パラメータ、ユーザAの公開鍵をサーバS v 1に渡す。ユーザAは暗号化装置20を保持し、ユーザAの公開鍵と公開パラメータを用いて平文データを暗号化し、得られた暗号文データをサーバS v 1に送信する。サーバS v 2は再暗号化鍵生成装置30を保持し、ユーザAの秘密鍵、ユーザBの再暗号化鍵生成鍵、公開パラメータ、及び乱数を用いて再暗号化鍵を生成し、得られた再暗号化鍵をサーバS v 1に渡す。サーバS v 1は再暗号化装置40を保持し、サーバS v 2から受けたユーザAの公開鍵、公開パラメータ、及び再暗号化鍵に基づいて、ユーザAから受けた暗号文データを検証処理すると共に、ユーザAから受けた暗号文データを復号せずに再暗号化し、得られた再暗号文データをユーザBに渡す。ユーザBは復号装置50を保持し、ユーザBの秘密鍵と公開パラメータに基づいて、サーバS v 1から受けた再暗号文データを検証処理すると共に

、サーバS v 1 から受けた再暗号文データを復号処理して平文データを得る。なお、各エンティティ間のデータの授受は、有線通信又は無線通信等の電氣的な通信手段に限らず、例えば、再暗号化鍵生成鍵、再暗号化鍵、暗号文データ又は再暗号文データ等のデータを記憶した記憶媒体をオフラインで配送又は手渡しする物理的な通信手段を用いてもよい。あるいは、各エンティティ間のデータの授受は、電氣的な通信手段と、物理的な通信手段とを組合せて用いてもよい。

[0050] また、電氣的な通信手段のみを用いる場合でも、以下に述べるように、当該エンティティ以外のエンティティを介在させても良い。あるエンティティ（以下、第1のエンティティと呼ぶ）から別のエンティティ（以下、第2のエンティティと呼ぶ）へデータ（例えば、再暗号化鍵生成鍵）を送る場合を考える。第1のエンティティとは、例えば、ユーザAである。第2のエンティティとは、例えば、グループ管理者である。第1のエンティティは、第2のエンティティ以外のエンティティ（以下、第3のエンティティと呼ぶ）へデータを送信する。第3のエンティティとは、例えば、サーバS v 1 である。次に、第2のエンティティは、当該データを第3のエンティティから受信する。

[0051] 図10において、ユーザAは鍵生成装置10を保持し、公開パラメータ、ユーザAの公開鍵と秘密鍵の組と再暗号化鍵生成鍵、及びユーザBの公開鍵と秘密鍵の組と再暗号化鍵生成鍵を生成する。ユーザAは、公開パラメータ、ユーザBの公開鍵と秘密鍵の組と再暗号化鍵生成鍵をユーザBに渡し、公開パラメータ、ユーザAの公開鍵をサーバS v 1 に渡す。ユーザAは暗号化装置20を保持し、ユーザAの公開鍵と公開パラメータを用いて平文データを暗号化し、得られた暗号文データをサーバS v 1 に送信する。ユーザAは再暗号化鍵生成装置30を保持し、ユーザAの秘密鍵、ユーザBの再暗号化鍵生成鍵、公開パラメータ、及び乱数を用いて再暗号化鍵を生成し、得られた再暗号化鍵をサーバS v 1 に渡す。サーバS v 1 は再暗号化装置40を保持し、ユーザAから受けたユーザAの公開鍵、公開パラメータ、及び再暗号

化鍵に基づいて、ユーザAから受けた暗号文データを検証処理すると共に、ユーザAから受けた暗号文データを復号せずに再暗号化し、得られた再暗号文データをユーザBに渡す。ユーザBは復号装置50を保持し、ユーザBの秘密鍵と公開パラメータに基づいて、サーバSv1から受けた再暗号文データを検証処理すると共に、サーバSv1から受けた再暗号文データを復号処理して平文データを得る。

[0052] 続いて、各装置10～50の構成を具体的に説明する。

[0053] 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、鍵生成部14、通信部15及び制御部16を備えている。

[0054] 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。

[0055] 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。

[0056] 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。

[0057] 鍵生成部14は、公開鍵・秘密鍵のペアと再暗号化鍵生成鍵を生成する。

[0058] 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、制御部16に制御されて一時データ記憶部12内の公開パラメータ、各30、50の公開鍵・秘密鍵のペア及び再暗号化鍵生成鍵を当該各装置30、50に送信する機能と、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に送信する機能と、制御部16に制御されて一時データ記憶部12内の公開パラメータと再暗号化鍵生成装置30の公開鍵を再暗号化装置40に送信する機能と、をもっている。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。

[0059] 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。

[0060] 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。

[0061] ここで、一時データ記憶部 21 は、鍵生成装置 10 から受けた公開パラメータと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を記憶する記憶装置である。

[0062] 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、鍵生成装置 10 から受けた公開パラメータ及び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 に書き込む機能や、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 に送信する機能をもっている。

[0063] 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っている。

[0064] 暗号文生成部 24 は、一時データ記憶部 21 から読み出した公開パラメータ及び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と、得られた暗号文データを一時データ記憶部 21 に書き込む機能とをもっている。

[0065] 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。

[0066] 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。

[0067] 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。

[0068] 一時データ記憶部 32 は、鍵生成装置 10 から受けた公開パラメータと復号装置 50 の再暗号化鍵生成鍵や、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。

- [0069] 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、鍵生成装置 10 から受けた公開パラメータ及び復号装置 50 の再暗号化鍵生成鍵を取得して一時データ記憶部 32 に書き込む機能や、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。
- [0070] 再暗号化鍵生成部 34 は、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 から読み出した公開パラメータ及び復号装置 50 の再暗号化鍵生成鍵（第 2 ユーザ装置の第 2 再暗号化鍵生成鍵）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と、この再暗号化鍵を一時データ記憶部 32 に書き込む機能とをもっている。
- [0071] 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。
- [0072] 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。
- [0073] なお、再暗号化鍵生成装置 30 は、鍵生成装置 10 から自装置 30 の再暗号化鍵生成鍵を受信する場合、鍵生成装置 10 から受けた自装置 30 の再暗号化鍵生成鍵を記憶する記憶装置である再暗号化鍵生成鍵記憶部をもつ（図示せず）。
- [0074] 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 46 を備えている。
- [0075] 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。
- [0076] 一時データ記憶部 42 は、鍵生成装置 10 から受けた公開パラメータと再暗号化鍵生成装置 30 の公開鍵や、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。
- [0077] 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

エースであり、例えば、鍵生成装置 10 から受けた公開パラメータ及び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 42 に書き込む機能や、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 に送出する機能と、制御部 46 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 に送信する機能とをもっている。

[0078] 再暗号化処理部 44 は、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、及び一時データ記憶部 42 から読み出した公開パラメータと再暗号化鍵生成装置 30 の公開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と、得られた再暗号文データを一時データ記憶部 42 に書き込む機能とをもっている。

[0079] 制御部 46 は、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。

[0080] 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 54、再暗号化鍵生成鍵記憶部 55、及び制御部 56 を備えている。

[0081] 秘密鍵記憶部 51 は、鍵生成装置 10 から受けた自装置 50 の秘密鍵を記憶する記憶装置である。

[0082] 一時データ記憶部 52 は、鍵生成装置 10 から受けた公開パラメータや、復号処理部 54 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。

[0083] 通信部 53 は、他の装置 10 ～ 40 と通信するための通信インタフェースであり、例えば、鍵生成装置 10 から受けた自装置 50 の秘密鍵を取得して秘密鍵記憶部 51 に書き込む機能と、鍵生成装置 10 から受けた公開パラメータを取得して一時データ記憶部 52 に書き込む機能と、再暗号化装置 40 から受けた再暗号化データを復号処理部 54 に送出する機能とをもっている。

[0084] 復号処理部 54 は、再暗号化装置 40 から再暗号文データを受けると、秘

密鍵記憶部 51 から読み出した当該復号装置 50 の秘密鍵（第 2 ユーザ装置の第 2 秘密鍵）、及び一時データ記憶部 52 から読み出した公開パラメータを用いて、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と、得られた平文データを一時データ記憶部 52 に書き込む機能とをもっている。

[0085] 再暗号化鍵生成鍵記憶部 55 は、鍵生成装置 10 から受けた自装置 50 の再暗号化鍵生成鍵を記憶する記憶装置である。

[0086] 制御部 56 は、図 6 に示す動作を実行するように、各部 51～55 を制御する機能をもっている。

[0087] なお、本実施形態では、例えば公開パラメータは各装置 10～50 の一時データ記憶部に記憶される。しかしこれに限らず、公開パラメータは各装置 10～50 の（一時データ記憶部とは別の）記憶部に記憶されていても良い。このように、各装置 10～50 の一時データ記憶部に記憶されるデータの内、一時的なデータとして扱わなくてもよいデータは、（一時データ記憶部とは別の）記憶部にそれぞれ記憶されていても良い。また、公開パラメータが複数の要素で構成されている場合、各装置 20～50 は、公開パラメータの各要素の内、後述する各処理においてそれぞれ必要な要素のみを取得しても良い。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。

[0088] 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。

[0089] 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。

[0090] （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。

[0091] 始めに、鍵生成装置 10 の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、公開パラメータ

[数1]

$$\text{par} = \{\lambda, p, G, G_T, g, g_1, g_2, g_3, g_4, g_5, u, v, \text{Sig}(\hat{G}, \hat{S}, \hat{V})\}$$

[0092] 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、位数 $p > 2^\lambda$ を満たす双線型写像群 (bilinear map groups) (G, G_T) を選択する。ここで、 p は整数である。 p は素数であっても良いし、合成数であっても良い。公開パラメータ生成部 13 は、 G の元 (げん) g, g_1, g_2, u, v を G からランダムに選択する。公開パラメータ生成部 13 は、 π を Z_p^* からランダムに選択し、 $g_3 = g^\pi, g_4 = g_1^\pi, g_5 = g_2^\pi$ を計算する。なお、 Z_p^* は Z_p かつ p と互いに素な整数の集合 ($= (Z/pZ)^*$) であり、 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。 g_3 は乱数 π とシステム固定値 g に基づく値である。 g_4 は乱数 π とシステム固定値 g_1 に基づく値である。 g_5 は乱数 π とシステム固定値 g_2 に基づく値である。さらに、公開パラメータ生成部 13 は、使い捨て署名 (one-time signature) アルゴリズム

[数2]

$\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ を生成する。また、使い捨て署名アルゴリズム $\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ (以

下、 $\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ を sig ともいう) における $\hat{G}$ は署名鍵と検証鍵のペア ($s s k, s$

$v k$) (両方とも使い捨ての鍵である) 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

。

[0093] 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。

[0094] 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。

[0095] 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。

[0096] 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。

[0097] 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。

[0098] 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 は、 G の元 g, g_1 に関するベキ指数であり、 β は、 G の元 g, g_2 に関するベキ指数である。ここで「 G の元 g, g_1 に関するベキ指数」とは、 G の元 g と g_1 との関係性を定めるベキ指数であり、 g を α 乗した元と g_1 とが G において等しくなるような値 α を表す。同様に、「 G の元 g, g_2 に関するベキ指数」とは、 G の元 g と g_2 との関係性を定めるベキ指数であり、 g を β 乗した元と g_2 とが G において等しくなるような値 β を表す。後述するように、 G を加法群として表現しても良いが、この場合、例えば、 G の元が楕円曲線上の点である場合は、上記ベキ指数をスカラーと読み替え、 α 乗を α 倍と読み替え、 β 乗を β 倍と読み替えれば良い。) 。

[0099] $e(g_1 g_2, g) = e(g, g_1 g_2) = e(g, g^\alpha \cdot g^\beta) = e(g, g^{\alpha + \beta}) = e(g, g)^{\alpha + \beta} = e(g, g)^\alpha \cdot e(g, g)^\beta$

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。

[0100] 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。例えば、 G の元が楕円曲線上の点であり、 G_T の元が有限体上の元であっても良い。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。この場合、後述する各処理における G の各元を、 G_1 の元又は G_2 の元と適宜書き換えればよい。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。

[0101] 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 $p a r$ 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 $p a r = (\lambda, p, G, G_T, g, g_1, g_2, g_3, g_4, g_5, u, v, Sig)$ を公開する(ST2)。なお、ステップ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、ステップST1及びステップST2をスキップしても良い。

[0102] また、鍵生成部14は、再暗号化鍵生成装置30の識別情報を i としたとき、 Z_p^* の元 x_i, y_i, z_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $s k_i = (x_i, y_i, z_i)$ とする。そして、鍵生成部14は、この秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成装置30の公開鍵 $p k_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i})$ を生成する。ここで、

[数3]

$$\begin{aligned} X_i &= g^{x_i}, & Y_{1i} &= g_1^{y_i}, & Y_{2i} &= g_2^{y_i}, \\ Z_i &= g^{z_i}, & Z_{1i} &= g_1^{z_i} \end{aligned}$$

[0103] である。なお、後述する式(a2')を用いた検証処理を行わない場合には

、データ Y_{2i} を省略してもよい。すなわち、公開鍵 pk_i は、データ X_i 、 Y_{1i} 、 Z_i 、 Z_{1i} を含んでいればよい。

[0104] さらに、鍵生成部 14 は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = (X_{3i}, Y_{5i})$ を生成する (ST3)。ここで、
[数4]

$$X_{3i} = g_3^{X_i}, \quad Y_{5i} = g_5^{Y_i}$$

[0105] である。

[0106] 続いて、鍵生成部 14 は、生成した公開鍵・秘密鍵のペアと再暗号化鍵生成鍵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 sk_i と再暗号化鍵生成鍵 rk_i を再暗号化鍵生成装置 30 に送信する (ST4)。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 (ST5)。

[0107] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、 Z_p^* の元 x_j 、 y_j 、 z_j を Z_p^* からランダムに選択し、復号装置 50 の秘密鍵 $sk_j = (x_j, y_j, z_j)$ とする。そして、鍵生成部 14 は、この秘密鍵 sk_j と公開パラメータ par を用いて復号装置 50 の公開鍵 $pk_j = (X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j})$ を生成する。ここで、
[数5]

$$X_j = g^{X_j}, \quad Y_{1j} = g_1^{Y_j}, \quad Y_{2j} = g_2^{Y_j}, \\ Z_j = g^{Z_j}, \quad Z_{1j} = g_1^{Z_j}$$

[0108] である。前述同様に、後述する式 (a2') を用いた検証処理を行わない場合には、データ Y_{2j} を省略してもよい。すなわち、公開鍵 pk_j は、データ X_j 、 Y_{1j} 、 Z_j 、 Z_{1j} を含んでいればよい。

[0109] さらに、鍵生成部 14 は、秘密鍵 sk_j と公開パラメータ par を用いて再

暗号化鍵生成鍵 $r k_j = (X_{3j}, Y_{5j})$ を生成する (ST6)。ここで、
[数6]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

[0110] である。

[0111] 続いて、鍵生成部14は、生成した公開鍵・秘密鍵のペアと再暗号化鍵生成鍵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 $s k_j$ と再暗号化鍵生成鍵 $r k_j$ を復号装置50に送信する (ST7)。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 (ST8)。また、所望により、暗号化装置20の秘密鍵 $s k_h$ 、公開鍵 $p k_h$ 、及び再暗号化鍵生成鍵 $r k_h$ についても各ステップST6～ST8と同様の処理を実行して暗号化装置20に秘密鍵 $s k_h$ と再暗号化鍵生成鍵 $r k_h$ を送信し、公開鍵 $p k_h$ を公開してもよい。また、鍵生成装置10は、暗号化装置20、再暗号化鍵生成装置30、又は復号装置50に、(再暗号化鍵生成鍵を送信せず) 秘密鍵のみを送信しても良い。また、鍵生成装置10は、暗号化装置20、再暗号化鍵生成装置30、又は復号装置50に、鍵セットアップ処理において生成された全ての公開鍵の内、一部又は全部の公開鍵を送信しても良い。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。

[0112] 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、各ステップST2、ST5、ST8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。

[0113] (2) 暗号化処理は、暗号化装置20により、図3及び以下の各ステップST21～ST24に示すように実行される。なお、暗号化装置20は、再暗号化鍵生成装置30の公開鍵 $p k_i$ を一時データ記憶部21に既に記憶していると想定しているが、もし暗号化装置20が再暗号化鍵生成装置30の公開鍵 $p k_i$ を未だ取得していない場合は、暗号化装置20は、後述するステップST22の前に、再暗号化鍵生成装置30の公開鍵 $p k_i$ を、例えば鍵生成

装置 10 から取得すれば良い。同様に、暗号化装置 20 は、公開パラメータ $p a r$ を一時データ記憶部 21 に既に記憶していると想定しているが、もし暗号化装置 20 が公開パラメータ $p a r$ を未だ取得していない場合は、暗号化装置 20 は、後述するステップ S T 21 の前に、公開パラメータ $p a r$ を、例えば鍵生成装置 10 から取得すれば良い。

[0114] 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 $p a r$ 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7]

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

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

[0115] を生成し (S T 21)、暗号化データ C_1 に検証鍵 $s v k$ をセットする ($C_1 = s v k$)。

[0116] 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。

[0117] 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 $p k_i$ 、及び公開パラメータ $p a r$ 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_{2Y} , C_{2Z} , C_{2Z1} , C_3 , C_4 を生成する (S T 22)。

[数8]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_5, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

ステップST22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 par における署名生成機能 $\hat{S}$ とステップST21で生成した署名鍵 sk により、使い捨て署名 σ を次式に示すように生成する(ST23)。

$$\sigma = \hat{S}(sk, (C_3, C_4))$$

ここで、関数 $\hat{S}$ の第1引数は署名鍵であり、第2引数は署名対象データである。

関数 $\hat{S}$

[0118] は、署名鍵と署名対象データを入力として、署名を出力する。

[0119] 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。

[0120] 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、後述するステップST41における検証処理を省略する場合、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。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。

[0121] 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(ST24)。

[0122] 以上により、暗号化処理が完了する。

[0123] (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

以下の各ステップST31～ST33に示すように実行される。なお、再暗号化鍵生成装置30は、公開パラメータ $p_a r$ を一時データ記憶部32に既に記憶していると想定しているが、もし再暗号化鍵生成装置30が公開パラメータ $p_a r$ を未だ取得していない場合は、再暗号化鍵生成装置30は、後述するステップST32の前に、公開パラメータ $p_a r$ を、例えば鍵生成装置10から取得すれば良い。

[0124] 今、復号装置50（図8の例では、例えばユーザA）が、再暗号化鍵生成装置30（図8の例では、グループ管理者）宛の暗号文を、復号装置50（図8の例では、例えばユーザA）宛の暗号文に再暗号化すること（つまり、暗号文の復号権限のユーザAへ移譲すること）を承諾したとする。復号装置50は、再暗号化鍵生成装置30に、復号装置50の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置50の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部32に書き込む（ST31）。なお、ステップST31において、（復号装置50ではなく）鍵生成装置10が再暗号化鍵生成装置30に再暗号化鍵生成鍵 $r k_j$ を送信しても良い。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。

[0125] ここで、一時データ記憶部32について、図11に示すように、再暗号化鍵生成装置30は、一時データ記憶部32の中に公開パラメータ記憶部321と再暗号化鍵生成鍵記憶部322を保持し、公開パラメータ $p_a r$ を公開パラメータ記憶部321に記憶し、復号装置50の再暗号化鍵生成鍵 $r k_j$ を再暗号化鍵生成鍵記憶部322に記憶しても良い。また、公開パラメータ $p_a r$ を記憶する公開パラメータ記憶部321は、一時データ記憶部32の外にあっても良い。また、再暗号化鍵生成鍵 $r k_j$ を記憶する再暗号化鍵生成鍵記憶部322は、一時データ記憶部32の外にあっても良い。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。また、通信部33は、前述したステップST4のとき、再暗号化鍵生成装置30の秘密鍵 $s k_j$ 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。

[0126] 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。

[0127] 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 $s k_i$ 、一時データ記憶部 32 内の復号装置 50 の再暗号化鍵生成鍵 $r k_j$ 、及び公開パラメータ $p a r$ を用いて、再暗号化鍵 R_{ij} を次式に示すように生成する (S T 32)。

[0128] $R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$

ここで、

[数9]

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}.$$

[0129] である。なお、上式では、 $g_2 = g^\beta$ と書き替えて表記している。

[0130] 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 (S T 33)。

[0131] 以上により、再暗号化鍵生成処理が完了する。

[0132] (4) 再暗号化処理は、再暗号化装置 40 により、図 5 及び以下の各ステップ S T 41 ~ S T 43 に示すように実行される。なお、再暗号化装置 40 は、再暗号化鍵生成装置 30 の公開鍵 $p k_i$ を一時データ記憶部 42 に既に記

憶していると想定しているが、もし再暗号化装置40が再暗号化鍵生成装置30の公開鍵 $p k_i$ を未だ取得していない場合は、再暗号化装置40は、後述するステップST41の前に、再暗号化鍵生成装置30の公開鍵 $p k_i$ を、例えば再暗号化鍵生成装置30から取得すれば良い。同様に、再暗号化装置40は、公開パラメータ $p a r$ を一時データ記憶部42に既に記憶していると想定しているが、もし再暗号化装置40が公開パラメータ $p a r$ を未だ取得していない場合は、再暗号化装置40は、後述するステップST41の前に、公開パラメータ $p a r$ を、例えば鍵生成装置10から取得すれば良い。

[0133] 再暗号化装置40の通信部43は、ステップST24で送信された暗号文データ C_i と、ステップST33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。

[0134] 再暗号化処理部44は、公開パラメータ $p a r$ と再暗号化鍵生成装置30の公開鍵 $p k_i$ を用い、一時データ記憶部42内の暗号文データ C_i を次の検証式により検証する(ST41)。

[数10]

$$\begin{aligned} e(C_{2X}, u^{C_1} \cdot v) &= e(X_i, C_4), \\ e(C_{2Y}, u^{C_1} \cdot v) &= e(Y_{1i}, C_4), \\ e(C_{2Z}, u^{C_1} \cdot v) &= e(Z_i, C_4), \\ e(C_{2Z1}, u^{C_1} \cdot v) &= e(Z_{1i}, C_4), \\ \hat{V}(C_1, \sigma, (C_3, C_4)) &= 1. \end{aligned} \quad \dots (a1)$$

ここで、関数 $\hat{V}$ の第1引数は検証鍵であり、第2引数は署名であり、第3引数は署名

対象データである。また、関数 $\hat{V}$

[0135] は、検証鍵を用いて、署名検証データに対する署名を検証し、署名が正当で

あると判定した場合は“1”を出力し、正当でないと判定した場合は“1”以外（例えば“0”）を出力する。

[0136] 従って、式（a 1）の5番目の検証式は、暗号化データ C_1 を検証鍵として用いて、署名対象データである暗号化データ C_3 、 C_4 に対する使い捨て署名 σ を検証し、使い捨て署名 σ が正当であると判定されることを表す。

[0137] ここで、式（a 1）の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。

[0138] 検証が成功した場合（又はステップS T 4 1の検証処理をスキップした場合）、再暗号化パラメータ生成部4 5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4 4に送出する。

[0139] 再暗号化処理部4 4は、これらの乱数 s 、 t 、 k 、一時データ記憶部4 2に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ij} 、再暗号化鍵生成装置3 0の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ 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_{5X} 、 C_{5Y} 、 C_{5Z} を生成する（S T 4 2）。

[数11]

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

[0140] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C'_{2X} \sim C_{5Z}$ 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 $C_j = (C_1, C'_{2X}, C''_{2X}, C'_{2Y}, C''_{2Y}, C'_{2Z}, C''_{2Z}, C'_{2Z1}, C''_{2Z1}, C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ 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4 2に書き込む。なお、再暗号文データ $C_j = (C_1, C'_{2X}, C''_{2X}, C'_{2Y}, C''_{2Y}, C'_{2Z}, C''_{2Z}, C'_{2Z1}, C''_{2Z1},$

$C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma$) は、後述する復号処理におけるステップ S T 5 1 の検証処理を省略する場合、復号に用いない検証用データ ($C_1, C_{2X}', C_{2Y}', C_{2Z}', C_{2Z1}', C_4, \sigma$) 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 ($C_{2X}', C_{2Y}', C_{2Z}', C_{2Z1}'$) を生成する処理も省略される。

[0141] いずれにしても通信部 4 3 は、制御部 4 6 に制御されて一時データ記憶部 4 2 内の再暗号文データ C_j を復号装置 5 0 に送信する (S T 4 3)。

[0142] 以上により、再暗号化処理が完了する。

[0143] なお、再暗号化処理部 4 4 は、ステップ S T 4 1 の検証処理を省略し、ステップ S T 4 2 の再暗号化データ生成処理を行ってもよい。また、暗号文データ C_i に検証用データ (C_1, C_4, σ) が含まれていない場合も、再暗号化処理部 4 4 は、ステップ S T 4 1 の検証処理を省略し、ステップ S T 4 2 の再暗号化データ生成処理を行う。

[0144] (5) 復号処理は、復号装置 5 0 により、図 6 及び以下のステップ S T 5 1 及び S T 5 2 に示すように実行される。なお、復号装置 5 0 は、公開パラメータ $p a r$ を一時データ記憶部 5 2 に既に記憶していると想定しているが、もし復号装置 5 0 が公開パラメータ $p a r$ を未だ取得していない場合は、復号装置 5 0 は、後述するステップ S T 5 1 の前に、公開パラメータ $p a r$ を、例えば鍵生成装置 1 0 から取得すれば良い。

[0145] 復号装置 5 0 の通信部 5 3 は、ステップ S T 4 3 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 5 2 に書き込む。

[0146] 復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と一時データ記憶部 5 2 内の公開パラメータ $p a r$ を用い、一時データ記憶部 5 2 内の再暗号文データ C_j を次の検証式により検証する (S T 5 1)。

[数12]

$$\begin{aligned}
e(C''_{2X}, u^{C_1} \cdot v) &= e(C'_{2X}, C_4), \\
e(C''_{2Y}, u^{C_1} \cdot v) &= e(C'_{2Y}, C_4), \\
e(C''_{2Z}, u^{C_1} \cdot v) &= e(C'_{2Z}, C_4), \\
e(C''_{2Z1}, u^{C_1} \cdot v) &= e(C'_{2Z1}, C_4), \\
e(C_{5Z}, C'_{2Z}) &= e(C_{5X}, C'_{2X}) \cdot e(g_2, g_3)^{y_j}, \\
e(C_{5Z}, C'_{2Z1}) &= e(C_{5Y}, C'_{2Y}) \cdot e(g, g_4)^{x_j}, \\
\hat{V}(C_1, \sigma, (C_3, C_4)) &= 1.
\end{aligned}
\quad \dots (a2)$$

ここで、式 (a2) の5番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z}) = e(C_{5X}, C'_{2X}) \cdot e(g_5, g)^{y_j}.$$

また、式 (a2) の5番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z}) = e(C_{5X}, C'_{2X}) \cdot e(Y_{2j}, g_3). \quad \dots (a2')$$

この場合、復号処理部54は、自装置50の公開鍵 $p k_j$ を用いて検証を行う。

また、式 (a2) の6番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z1}) = e(C_{5Y}, C'_{2Y}) \cdot e(g_3, g_1)^{x_j}.$$

また、式 (a2) の6番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z1}) = e(C_{5Y}, C'_{2Y}) \cdot e(X_j, g_4).$$

この場合、復号処理部54は、自装置50の公開鍵 $p k_j$ を用いて検証を行う。

[0147] 式 (a2) の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。

[0148] 検証が成功した場合（又はステップST51の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 $s k_j$ と一時データ記憶部52内の公開パラメータ $p a r$ 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 5 2)。

[数13]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(x_j + \beta y_j + \theta)/z_k}, g^{z_k r k})}{e(g^{\pi(x_j + \theta)/x_i s}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi(x_j + \beta y_j + \theta)/z_k}, g^{\alpha z_k r k})}{e(g^{\pi(\beta y_j + \theta)/y_i t}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(x_j + \beta y_j + \theta)}, g^r)}{e(g^{\pi(x_j + \theta)}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi(x_j + \beta y_j + \theta)}, g^{\alpha r})}{e(g^{\pi(\beta y_j + \theta)}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0149] 以上により、復号処理が完了する。

[0150] なお、復号処理部 5 4 は、ステップ S T 5 1 の検証処理を省略し、ステップ S T 5 2 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 (C_1 , C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_4 , σ) が含まれていない場合も、復号処理部 5 4 は、ステップ S T 5 1 の検証処理を省略し、ステップ S T 5 2 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。

[0151] 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。

[0152] 上述したように本実施形態によれば、再暗号化鍵 R_{ij} を再暗号化鍵生成鍵 r_{k_j} に基づいて生成する構成により、復号装置 50（第2ユーザ装置）のユーザの許可なしに、再暗号化鍵が生成されることがない。言い換えると、移譲先（図8の例では、例えばユーザA）が再暗号化鍵生成鍵を移譲元（図8の例では、グループ管理者）に通知しなければ再暗号化鍵が生成され得ない。このため、移譲先の承諾なく再暗号化（つまり、暗号文の復号権限の当該移譲先への移譲）を行わないようにすることができるので、安全なファイル共有を実現することができる。

[0153] また、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。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。

[0154] 補足すると、従来は、サーバの運営者、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_{AB} ）、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_{AE} ）を、移譲元であるユーザAの許可なく第三者が計算できてしまう（つまり、復号権限を移譲元の許可なく再移譲されてしまう）不都合がある。

[0155] しかしながら、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、サーバの運営者、ユーザB及びユーザE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。

[0156] [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。

[0157] 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')。

[0158] 復号装置50は、公開パラメータ $p_a r$ と自装置50の秘密鍵 $s k_i$ を用いて、暗号化装置20において生成された暗号文データ C_i を次の検証式により検証する(ST51')。

[数14]

$$\begin{aligned} e(C_{2X}, u^{C_1} \cdot v) &= e(g, C_4)^{x_i}, \\ e(C_{2Y}, u^{C_1} \cdot v) &= e(g_1, C_4)^{y_i}, \\ e(C_{2Z}, u^{C_1} \cdot v) &= e(g, C_4)^{z_i}, \\ e(C_{2Z1}, u^{C_1} \cdot v) &= e(g_1, C_4)^{z_i}, \\ \hat{V}(C_1, \sigma, (C_3, C_4)) &= 1. \end{aligned}$$

… (a3)

[0159] なお、復号装置50は、公開パラメータ $p_a r$ と自装置50の公開鍵 $p k_i$ を用いて、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と同様に検証しても良い。

[0160] 式(a3)の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。

[0161] 検証が成功した場合（又はステップST51'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（ST52'）。

[数15]

$$m = C_3 / e(g_4 g_5, C_{2X})^{\frac{1}{x_i}}$$

なお、上式は、

$$(g_4 g_5)^{\frac{1}{x_i}}$$

を予め計算しておき、それを用いて、

$$m = \frac{C_3}{e\left((g_4 g_5)^{\frac{1}{x_i}}, C_{2X}\right)}$$

と計算しても良い。これにより復号時の計算処理負荷を削減することができる。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。

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。

$$\begin{aligned} m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, C_{2X})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g)^r = m. \end{aligned}$$

[0162] [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。

[0163] 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 ($C_1 = s_v, k$)。

[0164] 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。

[0165] 暗号文生成部 24 は、これらの乱数 r, s, t, k, θ 、復号装置 50 の公開鍵 p, k_j 、及び公開パラメータを用いて、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 $C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4$ を生成する (ST 22')。

[数16]

$$\begin{aligned} C_{2X}' &= Y_{2j}^s, C_{2X}'' = Y_{2j}^{rs}, C_{2Y}' = X_j^t, C_{2Y}'' = X_j^{rt}, \\ C_{2Z}' &= Y_{2j}^k, C_{2Z}'' = Y_{2j}^{rk}, C_{2Z1}' = X_j^k, C_{2Z1}'' = X_j^{rk}, \\ C_3 &= e(g_4 g_5, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r, \\ C_{5X} &= (g_4 \cdot g_3^\theta)^{\frac{1}{s}}, C_{5Y} = g_3^{\frac{\theta+1}{t}}, C_{5Z} = (g_4 \cdot g_3^{\theta+1})^{\frac{1}{k}} \end{aligned}$$

[0166] 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 (ST 23')。

[0167] 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_{2Y}'' , C_{5X} , C_{5Y} , C_{5Z} , C_3 , C_4 , σ) 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。

[0168] 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 (ST24')。

[0169] 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 (ST51')。検証が成功した場合 (又はステップ ST51' の検証処理をスキップした場合)、復号装置 50 は、自装置 50 の秘密鍵 s_k と公開パラメータ $p_a r$ 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 (ST52')。

[数17]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(1+\alpha+\theta)/k}, g^{\beta y_j r k})}{e(g^{\pi(\alpha+\theta)/s}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi(1+\alpha+\theta)/k}, g^{x_j r k})}{e(g^{\pi(\theta+1)/t}, g^{x_j r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(1+\alpha+\theta)}, g^{\beta r})}{e(g^{\pi(\alpha+\theta)}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{\pi(1+\alpha+\theta)}, g^r)}{e(g^{\pi(\theta+1)}, g^r)} \right) \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0170] [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。

[0171] [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_6 を含める場合、第 1 の実施形態において、 $g_2 = g_2 g_6$ として、 g_2 を $g_2 g_6$ 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_6 , g_7 を含める場合、第 1 の実施形態において、 $g_1 = g_1 g_6$, $g_2 = g_2 g_7$ として、 g_1 を $g_1 g_6$ に、 g_2 を $g_2 g_7$ 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。

[0172] [変形例 5]

第 1 の実施形態では、公開パラメータに (g_3, g_4, g_5) の組が一つ含まれる例を説明したが、これに限らず、公開パラメータに (g_3, g_4, g_5) の組が複数含まれていても良い。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。

[0173] 以下、本変形例における鍵セットアップ処理、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し、第 1 の実施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。

[0174] (1) 鍵セットアップ処理

鍵生成装置 10 の公開パラメータ生成部 13 は、 $\pi_1, \pi_2, \dots, \pi_N$ を Z_p^* からランダムに選択し、次式により示される $A_1, A_2, \dots, A_N$ を計算する。

[数18]

$$A_n = (\text{tag}_n, g_{3,n}, g_{4,n}, g_{5,n}) \quad (n = 1, 2, \dots, N)$$

$$g_{3,n} = g^{\pi_n}, \quad g_{4,n} = g_1^{\pi_n}, \quad g_{5,n} = g_2^{\pi_n}$$

[0175] ここで、 N は自然数である。また、 tag_n ($n=1, 2, \dots, N$) は A_n の識別情報である。 tag_n は数値であっても良いし、文字列であっても良い。また、 A_n の(tag_n 以外の)要素そのものを tag_n として用いて良い。この場合、 A_n の要素として tag_n を追加する必要はなく、 tag_n を生成する処理も行わなくて良い。

[0176] 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、公開パラメータ

[数19]

$$\text{par} = \{\lambda, p, G, G_T, g, g_1, g_2, \{A_1, A_2, \dots, A_N\}, u, v, \text{Sig}(\hat{G}, \hat{S}, \hat{V})\}$$

[0177] を生成する、又は外部から入手する(ST1')。

[0178] 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 $\text{par} = (\lambda, p, G, G_T, g, g_1, g_2, A_1, A_2, \dots, A_N, u, v, \text{Sig})$ を公開する(ST2')。

[0179] また、鍵生成部14は、再暗号化鍵生成装置30の識別情報を i 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 $\text{sk}_i = (x_i, y_i, z_i)$ と公開パラメータ par を用いて再暗号化鍵生成装置30の公開鍵 $\text{pk}_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i})$ を生成する。ここで、

[数20]

$$X_i = g^{x_i}, \quad Y_{1i} = g_1^{y_i}, \quad Y_{2i} = g_2^{y_i},$$

$$Z_i = g^{z_i}, \quad Z_{1i} = g_1^{z_i}$$

[0180] である。なお、後述する式 (a 7') を用いた検証処理を行わない場合には、データ Y_{2i} を省略してもよい。すなわち、公開鍵 pk_i は、データ X_i , Y_{1i} , Z_i , Z_{1i} を含んでいればよい。

[0181] さらに、鍵生成部 14 は、秘密鍵 sk_i と公開パラメータ par を用いて、次式により示される再暗号化鍵生成鍵 $rk_{i,1}$, $rk_{i,2}$, ..., $rk_{i,N}$ を生成する (ST3')。

[数21]

$$rk_{i,n} = (X_{3i,n}, Y_{5i,n}) \quad (n = 1, 2, \dots, N)$$

ここで、

$$X_{3i,n} = g_{3,n}^{x_i}, \quad Y_{5i,n} = g_{5,n}^{y_i}$$

[0182] である。

[0183] 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 sk_i と再暗号化鍵生成鍵 $rk_{i,1}$, $rk_{i,2}$, ..., $rk_{i,N}$ を再暗号化鍵生成装置 30 に送信する (ST4')。なお、通信部 15 は、 $rk_{i,1}$, $rk_{i,2}$, ..., $rk_{i,N}$ に代えて、 $(tag_1, rk_{i,1})$, $(tag_2, rk_{i,2})$, ..., $(tag_N, rk_{i,N})$ を再暗号化鍵生成装置 30 に送信しても良い。

[0184] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、復号装置 50 の秘密鍵 $sk_j = (x_j, y_j, z_j)$ を生成し、この秘密鍵 sk_j を用いて復号装置 50 の公開鍵 $pk_j = (X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j})$ を生成する。ここで、

[数22]

$$\begin{aligned} X_j &= g^{x_j}, \quad Y_{1j} = g_1^{y_j}, \quad Y_{2j} = g_2^{y_j}, \\ Z_j &= g^{z_j}, \quad Z_{1j} = g_1^{z_j} \end{aligned}$$

[0185] である。前述同様に、後述する式 (a 7') を用いた検証処理を行わない場

合には、データ Y_{2j} を省略してもよい。すなわち、公開鍵 pk_j は、データ X_j , Y_{1j} , Z_j , Z_{1j} を含んでいればよい。

[0186] さらに、鍵生成部 14 は、秘密鍵 sk_j と公開パラメータ par を用いて、次式により示される再暗号化鍵生成鍵 $rk_{j,1}$, $rk_{j,2}$, ..., $rk_{j,N}$ を生成する (ST6')。

[数23]

$$rk_{j,n} = (X_{3j,n}, Y_{5j,n}) \quad (n = 1, 2, \dots, N)$$

ここで、

$$X_{3j,n} = g_{3,n}^{x_j}, \quad Y_{5j,n} = g_{5,n}^{y_j}$$

[0187] である。

[0188] 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 sk_j と再暗号化鍵生成鍵 $rk_{j,1}$, $rk_{j,2}$, ..., $rk_{j,N}$ を復号装置 50 に送信する (ST7')。なお、通信部 15 は、 $rk_{j,1}$, $rk_{j,2}$, ..., $rk_{j,N}$ に代えて、 $(tag_1, rk_{j,1})$, $(tag_2, rk_{j,2})$, ..., $(tag_N, rk_{j,N})$ を復号装置 50 に送信しても良い。

[0189] (2) 暗号化処理

暗号化装置 20 の暗号化パラメータ生成部 23 は、第 1 の実施形態のステップ ST21 と同様に、使い捨て署名における署名鍵 ssk と検証鍵 svk の鍵ペア (ssk, svk) を生成し (ST21')、暗号化データ C_1 に検証鍵 svk をセットする ($C_1 = svk$)。

[0190] 暗号文生成部 24 は、公開パラメータ par の要素である A_1 , A_2 , ..., A_N の中から一つを選択する。以下、 A_n が選択されたとする。

[0191] 暗号文生成部 24 は、乱数 r 、再暗号化鍵生成装置 30 の公開鍵 pk_i 、及び公開パラメータ par 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_{2Y} , C_{2Z} , C_{2Z1} , C_3 , C_4 を生成する (ST22')。

[数24]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_3 = e(g_{4,n}g_{5,n}, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

ステップST22の終了後、暗号文生成部24は、 A_n の識別情報 tag_n 及び暗号化

データ C_3, C_4 に対し、公開パラメータ par における署名生成機能 $\hat{S}$ とステップST

21' で生成した署名鍵 ssk により、使い捨て署名 σ を次式に示すように生成する (ST23')。

$$\sigma = \hat{S}(ssk, (tag_n, C_3, C_4))$$

[0192] なお、暗号文生成部24は、署名対象データとして A_n の識別情報 tag_n を含めず、暗号化データ C_3, C_4 を署名対象データとして、使い捨て署名 σ を生成しても良い。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。

[0193] しかる後、暗号文生成部24は、上記全ての暗号化データ $C_1 \sim C_4$ 、使い捨て署名 σ 、及び A_n の識別情報 tag_n を含む暗号文データ $C_i = (C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, \sigma, tag_n)$ を生成する。

[0194] なお、暗号文データ $C_i = (C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, \sigma, tag_n)$ は、後述する復号処理におけるステップST41' 及びステップST51' の検証処理を省略する場合、復号に用いない検証用データ (C_1, C_4, σ, tag_n) 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。ただし、後述する変形例6における復号処理を行う場合は、暗号文生成部24は、暗号文データ C_i に A_n の識別情報 tag_n を付加する。

[0195] 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 (ST24')。

[0196] (3) 再暗号化鍵生成処理

復号装置50 (図8の例では、例えばユーザA) が、再暗号化鍵生成装置30 (図8の例では、グループ管理者) 宛の暗号文であり、かつ公開パラメ

ータ par の要素である A_n を用いて暗号化された暗号文を、復号装置 50（図 8 の例では、例えばユーザ A）宛の暗号文に再暗号化すること（つまり、 A_n を用いて暗号化された暗号文の復号権限のユーザ A へ移譲すること）を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、 A_n の識別情報 tag_n と復号装置 50 の再暗号化鍵生成鍵 $rk_{j,n}$ を送信する。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、 A_n の識別情報 tag_n と復号装置 50 の再暗号化鍵生成鍵 $rk_{j,n}$ を取得して一時データ記憶部 32 に書き込む（ST31'）。

[0197] 再暗号化鍵生成部 34 は、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 sk_i 、一時データ記憶部 32 内の A_n の識別情報 tag_n 、復号装置 50 の再暗号化鍵生成鍵 $rk_{j,n}$ 、及び公開パラメータ par を用いて、再暗号化鍵 $R_{ij,n}$ を次式に示すように生成する（ST32'）。

[数25]

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

ここで、

$$R_{ij1,n} = (X_{3j,n} \cdot g_{3,n}^{\theta})^{1/x_i} = g^{\frac{\pi_n(x_j + \theta)}{x_i}},$$

$$R_{ij2,n} = (Y_{5j,n} \cdot g_{3,n}^{\theta})^{1/y_i} = g^{\frac{\pi_n(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3,n} = (X_{3j,n} \cdot Y_{5j,n} \cdot g_{3,n}^{\theta})^{1/z_i} = g^{\frac{\pi_n(x_j + \beta y_j + \theta)}{z_i}}.$$

[0198] である。なお、上式では、 $g_2 = g^{\beta}$ と書き替えて表記している。

[0199] （４）再暗号化处理 再暗号化处理部 44 は、公開パラメータ par と再暗号化鍵生成装置 30 の公開鍵 pk_i を用い、一時データ記憶部 42 内の暗号

文データ C_i を次の検証式により検証する (S T 4 1')。

[数26]

$$\begin{aligned} e(C_{2X}, u^{C_1} \cdot v) &= e(X_i, C_4), \\ e(C_{2Y}, u^{C_1} \cdot v) &= e(Y_{1i}, C_4), \\ e(C_{2Z}, u^{C_1} \cdot v) &= e(Z_i, C_4), \\ e(C_{2Z1}, u^{C_1} \cdot v) &= e(Z_{1i}, C_4), \\ \hat{V}(C_1, \sigma, (\text{tag}_n, C_3, C_4)) &= 1. \end{aligned} \quad \dots (a 4)$$

[0200] なお、式 (a 4) の5番目の検証式について、使い捨て署名 σ の署名対象データとして A_n の識別情報 tag_n が含まれていない場合、署名対象データを暗号化データ C_3 , C_4 として使い捨て署名 σ の検証を行う。後述の使い捨て署名 σ の検証処理においても同様である。

[0201] ここで、式 (a 4) の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。

[0202] 検証が成功した場合 (又はステップ S T 4 1' の検証処理をスキップした場合)、再暗号化パラメータ生成部 4 5 は、3つの乱数 $s, t, k \in Z_p^*$ を生成して再暗号化処理部 4 4 に送出する。

[0203] 再暗号化処理部 4 4 は、これらの乱数 s, t, k 、一時データ記憶部 4 2 に記憶されている、暗号文データ C_i 、再暗号化鍵 $R_{ij,n}$ 、再暗号化鍵生成装置 3 0 の公開鍵 pk_i 、及び公開パラメータ par を用いて、次式に示すように、再暗号化データ $C'_{2X}, C'_{2X'}, C'_{2Y}, C'_{2Y'}, C'_{2Z}, C'_{2Z'}, C'_{2Z1}, C'_{2Z1'}, C'_{5X}, C'_{5Y}, C'_{5Z}$ を生成する (S T 4 2')。

[数27]

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

[0204] なお、再暗号化処理部44は、ステップST24'で送信された暗号文データC_jに含まれるA_nの識別情報tag_nにより、ステップST42'において用いるべき再暗号化鍵R_{ij,n}を選択するようにしても良い。

[0205] ステップST42'の終了後、再暗号化処理部44は、上記全ての再暗号化データC_{2X'}～C_{5Z}を、暗号文データC_j内の暗号化データC_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}と置換し、さらに、ステップST24'で送信された暗号文データC_jに含まれるA_nの識別情報tag_nを、再暗号文データC_jに付加する。すなわち、C_j = (C₁, C_{2X'}, C_{2X''}, C_{2Y'}, C_{2Y''}, C_{2Z'}, C_{2Z''}, C_{2Z1'}, C_{2Z1''}, C_{5X}, C_{5Y}, C_{5Z}, C₃, C₄, σ, tag_n)である。再暗号化処理部44は、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。

[0206] なお、再暗号文データC_j = (C₁, C_{2X'}, C_{2X''}, C_{2Y'}, C_{2Y''}, C_{2Z'}, C_{2Z''}, C_{2Z1'}, C_{2Z1''}, C_{5X}, C_{5Y}, C_{5Z}, C₃, C₄, σ, tag_n)は、後述する復号処理におけるステップST51'の検証処理を省略する場合、復号に用いない検証用データ(C₁, C_{2X'}, C_{2Y'}, C_{2Z'}, C_{2Z1'}, C₄, σ, tag_n)を省略して、C_j = (C_{2X''}, C_{2Y''}, C_{2Z''}, C_{2Z1''}, C_{5X}, C_{5Y}, C_{5Z}, C₃)としてもよい。この場合、検証用データ(C_{2X'}, C_{2Y'}, C_{2Z'}, C_{2Z1'})を生成する処理も省略される。

[0207] いずれにしても通信部43は、制御部46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')。

[0208] (5) 復号処理

復号装置50の復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵sk_jと一時データ記憶部52内の公開パラメータparを用い、一時デ

ータ記憶部 5 2 内の再暗号文データ C_j を次の検証式により検証する (S T 5 1') 。

[数28]

$$\begin{aligned}
 e(C''_{2X}, u^{C_1} \cdot v) &= e(C'_{2X}, C_4), \\
 e(C''_{2Y}, u^{C_1} \cdot v) &= e(C'_{2Y}, C_4), \\
 e(C''_{2Z}, u^{C_1} \cdot v) &= e(C'_{2Z}, C_4), \\
 e(C''_{2Z1}, u^{C_1} \cdot v) &= e(C'_{2Z1}, C_4), \\
 e(C_{5Z}, C'_{2Z}) &= e(C_{5X}, C'_{2X}) \cdot e(g_2, g_{3,n})^{y_j}, \\
 e(C_{5Z}, C'_{2Z1}) &= e(C_{5Y}, C'_{2Y}) \cdot e(g, g_{4,n})^{x_j}, \\
 \hat{V}(C_1, \sigma, (\text{tag}_n, C_3, C_4)) &= 1. \quad \dots (a 7)
 \end{aligned}$$

ここで、式 (a 7) の 5 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z}) = e(C_{5X}, C'_{2X}) \cdot e(g_{5,n}, g)^{y_j}$$

また、式 (a 7) の 5 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z}) = e(C_{5X}, C'_{2X}) \cdot e(Y_{2j}, g_{3,n}) \quad \dots (a 7')$$

この場合、復号処理部 5 4 は、自装置 5 0 の公開鍵 $p k_j$ を用いて検証を行う。

また、式 (a 7) の 6 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z1}) = e(C_{5Y}, C'_{2Y}) \cdot e(g_{3,n}, g_1)^{x_j}$$

また、式 (a 7) の 6 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z1}) = e(C_{5Y}, C'_{2Y}) \cdot e(X_j, g_{4,n})$$

この場合、復号処理部 5 4 は、自装置 5 0 の公開鍵 $p k_j$ を用いて検証を行う。

[0209] なお、復号装置 5 0 の復号処理部 5 4 は、ステップ S T 4 3' で送信された再暗号文データ C_j に含まれる A_n の識別情報 tag_n により、公開パラメータ $p a r$ の要素である $A_1, A_2, \dots, A_N$ の中から、ステップ S T 5 1' にお

いて用いるべき A_n を選択するようにしても良い。

[0210] 復号装置 50 は、自装置 50 の秘密鍵 s_k と公開パラメータ $p_a r$ 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 (S T 5 2')。

[数29]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi_n(x_j + \beta y_j + \theta)/z_k}, g^{z_k r k})}{e(g^{\pi_n(x_j + \theta)/x_s}, g^{x_s r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi_n(x_j + \beta y_j + \theta)/z_k}, g^{\alpha z_k r k})}{e(g^{\pi_n(\beta y_j + \theta)/y_t}, g^{\alpha y_t r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi_n(x_j + \beta y_j + \theta)}, g^r)}{e(g^{\pi_n(x_j + \theta)}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi_n(x_j + \beta y_j + \theta)}, g^{\alpha r})}{e(g^{\pi_n(\beta y_j + \theta)}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_{4,n} g_{5,n}, g)^r / (e(g, g)^{\pi_n \beta r} \cdot e(g, g)^{\pi_n \alpha r}) = m. \end{aligned}$$

[0211] [変形例 6]

変形例 5 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、変形例5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。

[0212] 本変形例における暗号化処理と、変形例5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'）。

[0213] 復号装置50は、変形例1のステップST51'と同様に、暗号化装置20において生成された暗号文データ*C_i*を検証する（ST51'）。

[0214] 検証が成功した場合（又はステップST51'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵*s k_i*と公開パラメータ*p a r*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（ST52'）。

[数30]

$$m = C_3 / e(g_{4,n}g_{5,n}, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} & m \cdot e(g_{4,n}g_{5,n}, g)^r / e(g_{4,n}g_{5,n}, C_{2X})^{\frac{1}{x_i}} \\ &= m \cdot e(g_{4,n}g_{5,n}, g)^r / e(g_{4,n}g_{5,n}, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_{4,n}g_{5,n}, g)^r / e(g_{4,n}g_{5,n}, g)^r = m. \end{aligned}$$

[0215] なお、復号装置50の復号処理部54は、ステップST24'で送信された暗号文データ*C_i*に含まれる*A_n*の識別情報*t a g_n*により、公開パラメータ*p a r*の要素である*A₁*, *A₂*, ..., *A_n*の中から、ステップST52'において

用いるべき A_n を選択するようにしても良い。

[0216] [変形例 7]

変形例 6 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、変形例 5 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。

[0217] 暗号化装置 20 の暗号化パラメータ生成部 23 は、第 1 の実施形態のステップ 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 ($C_1 = s_v, k$)。

[0218] 暗号文生成部 24 は、公開パラメータ p, a, r の要素である $A_1, A_2, \dots, A_n$ の中から一つを選択する。以下、 A_n が選択されたとする。

[0219] 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。

[0220] 暗号文生成部 24 は、これらの乱数 r, s, t, k, θ 、復号装置 50 の公開鍵 p, k_j 、及び公開パラメータを用いて、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 $C'_{2X}, C''_{2X}, C'_{2Y}, C''_{2Y}, C'_{2Z}, C''_{2Z}, C'_{2Z1}, C''_{2Z1}, C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4$ を生成する $(ST 22')$ 。

[数 31]

$$\begin{aligned} C'_{2X} &= Y_{2j}^s, C''_{2X} = Y_{2j}^{rs}, C'_{2Y} = X_j^t, C''_{2Y} = X_j^{rt}, \\ C'_{2Z} &= Y_{2j}^k, C''_{2Z} = Y_{2j}^{rk}, C'_{2Z1} = X_j^k, C''_{2Z1} = X_j^{rk}, \\ C_3 &= e(g_{4,n} g_{5,n}, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r, \\ C_{5X} &= (g_{4,n} \cdot g_{3,n}^\theta)^{\frac{1}{s}}, C_{5Y} = g_{3,n}^{\frac{\theta+1}{t}}, C_{5Z} = (g_{4,n} \cdot g_{3,n}^{\theta+1})^{\frac{1}{k}} \end{aligned}$$

- [0221] ステップST22'の終了後、暗号文生成部24は、変形例5のステップST23'と同様に、使い捨て署名 σ を生成する(ST23')。
- [0222] 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 $C_j = (C_1, C_{2X}', C_{2X}''', C_{2Y}', C_{2Y}''', C_{2Z}', C_{2Z}''', C_{2Z1}', C_{2Z1}''', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma, tag_n)$ 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。
- [0223] 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(ST24')。
- [0224] 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 を変形例5のステップST51'と同様に検証する(ST51')。
- [0225] なお、復号装置50の復号処理部54は、ステップST24'で送信された暗号文データ C_j に含まれる A_n の識別情報 tag_n により、公開パラメータ par の要素である $A_1, A_2, \dots, A_N$ の中から、ステップST51'において用いるべき A_n を選択するようにしても良い。
- [0226] 検証が成功した場合（又はステップST51'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 sk_j と公開パラメータ par 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(ST52')。

[数32]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi_n(1+\alpha+\theta)/k}, g^{\beta y_j r k})}{e(g^{\pi_n(\alpha+\theta)/s}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi_n(1+\alpha+\theta)/k}, g^{x_j r k})}{e(g^{\pi_n(\theta+1)/t}, g^{x_j r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi_n(1+\alpha+\theta)}, g^{\beta r})}{e(g^{\pi_n(\alpha+\theta)}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{\pi_n(1+\alpha+\theta)}, g^r)}{e(g^{\pi_n(\theta+1)}, g^r)} \right) \right\} \\ &= m \cdot e(g_{4,n} g_{5,n}, g)^r / (e(g, g)^{\pi_n \beta r} \cdot e(g, g)^{\pi_n \alpha r}) = m. \end{aligned}$$

[0227] (第2の実施形態)

本実施形態では、第1の実施形態において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。鍵セットアップ処理、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。すなわち、定期的に時間パラメータLを変えて、暗号化処理、再暗号化鍵生成処理、及び再暗号化処理を行う。以下

、本実施形態における鍵セットアップ処理、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、前述の第1の実施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。

[0228] (1) 鍵セットアップ処理

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 $p a r$ を、第1の実施形態と同様に生成する、又は外部から入手する(ST1)。鍵生成部14は、再暗号化鍵生成装置30の識別情報を i としたとき、 Z_p^* の元 x_i, y_i, z_i, w_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $s k_i = (x_i, y_i, z_i, w_i)$ とする。そして、鍵生成部14は、この秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成装置30の公開鍵 $p k_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i}, W_i)$ を生成する。ここで、

[数33]

$$\begin{aligned} X_i &= g^{x_i}, & Y_{1i} &= g_1^{y_i}, & Y_{2i} &= g_2^{y_i}, \\ Z_i &= g^{z_i}, & Z_{1i} &= g_1^{z_i}, & W_i &= g^{w_i} \end{aligned}$$

[0229] である。なお、後述する式(a6')を用いた検証処理を行わない場合には、データ Y_{2i} を省略してもよい。すなわち、公開鍵 $p k_i$ は、 $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ を含んでいればよい。

[0230] さらに、鍵生成部14は、秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_i = (X_{3i}, Y_{5i})$ を生成する(ST3)。ここで、

[数34]

$$X_{3i} = g_3^{x_i}, \quad Y_{5i} = g_5^{y_i}$$

[0231] である。

[0232] また同様に、鍵生成部14は、復号装置50の識別情報を j としたとき、 Z_p^* の元 x_j, y_j, z_j, w_j を Z_p^* からランダムに選択し、復号装置50の秘密鍵 $s k_j = (x_j, y_j, z_j, w_j)$ とする。そして、鍵生成部14は、この秘密鍵

$s k_j$ と公開パラメータ $p a r$ を用いて復号装置 50の公開鍵 $p k_j = (X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j}, W_j)$ を生成する。ここで、

[数35]

$$\begin{aligned} X_j &= g^{x_j}, & Y_{1j} &= g_1^{y_j}, & Y_{2j} &= g_2^{y_j}, \\ Z_j &= g^{z_j}, & Z_{1j} &= g_1^{z_j}, & W_j &= g^{w_j} \end{aligned}$$

[0233] である。前述同様に、後述する式 (a 6') を用いた検証処理を行わない場合、データ Y_{2j} を省略してもよい。すなわち、公開鍵 $p k_j$ は、 $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$ を含んでいればよい。

[0234] さらに、鍵生成部 14 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = (X_{3j}, Y_{5j})$ を生成する (ST6)。ここで、

[数36]

$$X_{3j} = g_3^{x_j}, \quad Y_{5j} = g_5^{y_j}$$

[0235] である。

[0236] (2) 暗号化処理

第1の実施形態のステップ ST21と同様に、暗号化装置 20の暗号化パラメータ生成部 23は、 $(s s k, s v k)$ 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 ($C_1 = s v k$)。

[0237] 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。

[0238] 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 $p k_i$ 、公開パラメータ $p a r$ 、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 $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4$ を生成する (ST22)。

[数37]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_{2F} = F_i(L)^r, C_3 = e(g_4g_5, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

ここで、関数 $F_i(L)$ は次式により定義される。

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

[0239] 暗号化装置 20（又は後述する再暗号化鍵生成装置 30）による時間パラメータの取得方法として、例えば、以下の方法を用いれば良い。あるエンティティ（例えば、図 8 のサーバ Sv、サーバ Sv とは別のサーバ、ユーザ管理者、グループ管理者、ユーザ管理者やグループ管理者とは別の管理者、ユーザ A、ユーザ B、ユーザ B、又はユーザ A～C とは別のユーザ）が時間パラメータを生成する時間パラメータ生成装置（図示せず）を保持し、時間パラメータ生成装置が暗号化装置 20（又は再暗号化鍵生成装置 30）に時間パラメータを通知するようにしても良い。また、入力を時刻とし、出力を時間パラメータとする関数を定義し、時刻とその関数を用いて時間パラメータを生成しても良い。この場合、暗号化装置 20（又は再暗号化鍵生成装置 30）は、暗号化处理（再暗号化鍵生成処理）を行う時刻に基づいた情報（例えば、暗号化处理（再暗号化鍵生成処理）を行う日付を数値化した値）を入力とした上記関数の出力値を時間パラメータ L として用いれば良く、他の装置から時間パラメータを取得する必要はない。また、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、又は復号装置 50 が時間パラメータを生成し、（時間パラメータを生成する）当該装置以外の装置に時間パラメータを通知しても良い。また、再暗号化鍵生成装置 30 は、後述するように復号装置 50 の再暗号化鍵生成鍵を復号装置 50 から取得するが、この際に再暗号化鍵生成鍵に加えて時間パラメータも復号装置 50 から取得しても良い。この場合、復号装置 50 は、上述のいずれかの方法

により時間パラメータを取得すれば良い。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。

[0240] なお、時間パラメータは、必ずしも時刻や日付などの時間に関するパラメータである必要はなく、例えば、文字列を数値化したものであっても良いし、乱数などの数値であってても良い。同様に、上述した関数への入力は、文字列を数値化したもの、又は乱数などの数値であってても良い。このように、時間パラメータの数値は、時間に無関係であってても良い。これは後述する実施形態や変形例でも同様である。

[0241] ステップS T 2 2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p a rにおける署名生成機能[数38]

$\hat{S}$ とステップS T 2 1で生成した署名鍵s s kにより、使い捨て署名 σ を次式に示すように生成する(S T 2 3)。

$$\sigma = \hat{S}(ssk, (L, C_3, C_4))$$

[0242] なお、暗号文生成部24は、署名対象データとして時間パラメータLを含めず、暗号化データ C_3 、 C_4 を署名対象データとして、使い捨て署名 σ を生成しても良い。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。

[0243] 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 $C_i = (L, C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, \sigma)$ 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。

[0244] 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 2 4)。

[0245] (3) 再暗号化鍵生成処理

今、復号装置50(図8の例では、例えばユーザA)が、再暗号化鍵生成装置30(図8の例では、グループ管理者)宛の、時間パラメータの値とし

てLを用いて生成された暗号文を、復号装置50（図8の例では、例えばユーザA）宛の暗号文に再暗号化すること（つまり、暗号文の復号権限のユーザAへ移譲すること）を承諾したとする。復号装置50は、再暗号化鍵生成装置30に、復号装置50の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置50の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部32に書き込む（ST31）。

[0246] 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。

[0247] 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の再暗号化鍵生成鍵 $r k_j$ 、公開パラメータ $p a r$ 、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）。

[0248] $R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$

ここで、

[数39]

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i \delta_x}, R_{ijL5} = g_1^{y_i \delta_y} = g^{\alpha y_i \delta_y}$$

[0249] 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。

[0250] (4) 再暗号化处理

再暗号化装置40の再暗号化处理部44は、公開パラメータ $p a r$ 、一時データ記憶部42内の暗号文データ C_i に含まれている時間パラメータL、及

び再暗号化鍵生成装置 30 の公開鍵 pk_i を用い、一時データ記憶部 42 内の暗号文データ C_i を次の検証式により検証する (S T 4 1)。

[数40]

$$\begin{aligned} e(C_{2X}, u^{C_1} \cdot v) &= e(X_i, C_4), \\ e(C_{2Y}, u^{C_1} \cdot v) &= e(Y_{1i}, C_4), \\ e(C_{2Z}, u^{C_1} \cdot v) &= e(Z_i, C_4), \\ e(C_{2Z1}, u^{C_1} \cdot v) &= e(Z_{1i}, C_4), \\ e(C_{2F}, u^{C_1} \cdot v) &= e(F_i(L), C_4), \\ \hat{V}(C_1, \sigma, (L, C_3, C_4)) &= 1. \end{aligned} \quad \dots (a 5)$$

[0251] なお、式 (a 5) の 6 番目の検証式について、使い捨て署名 σ の署名対象データとして時間パラメータ L が含まれていない場合、署名対象データを暗号化データ C_3 , C_4 として使い捨て署名 σ の検証を行う。これは、後述の使い捨て署名 σ の検証処理においても同様である。

[0252] ここで、式 (a 5) の 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。

[0253] 検証が成功した場合 (又はステップ S T 4 1 の検証処理をスキップした場合)、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。

[0254] 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 に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ijL} 、再暗号化鍵生成装置 30 の公開鍵 pk_i 、及び公開パラメータ par 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 (S T 4 2)

。

[数41]

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

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}$$

[0255] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_{2X}' \sim C_{5FY}$ 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 $C_j = (L, C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部4 2に書き込む。

[0256] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する(S T 4 3)。

[0257] (5) 復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 s_{kj} と一時データ記憶部5 2内の公開パラメータ p_{ar} を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する(S T 5 1)。

[数42]

$$\begin{aligned}
e(C_{2X}'', u^{C_1} \cdot v) &= e(C_{2X}', C_4), \\
e(C_{2Y}'', u^{C_1} \cdot v) &= e(C_{2Y}', C_4), \\
e(C_{2Z}'', u^{C_1} \cdot v) &= e(C_{2Z}', C_4), \\
e(C_{2Z1}'', u^{C_1} \cdot v) &= e(C_{2Z1}', C_4), \\
e(C_{2F}'', u^{C_1} \cdot v) &= e(C_{2F}', C_4), \\
e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') &= e(C_{5X}, C_{2X}') \cdot e(g_2, g_3)^{y_j}, \\
e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') &= e(C_{5Y}, C_{2Y}') \cdot e(g, g_4)^{x_j}, \\
\hat{V}(C_1, \sigma, (L, C_3, C_4)) &= 1. \quad \dots (a6)
\end{aligned}$$

ここで、式 (a 6) の 6 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') = e(C_{5X}, C_{2X}') \cdot e(g_5, g)^{y_j}.$$

また、式 (a 6) の 6 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') = e(C_{5X}, C_{2X}') \cdot e(Y_{2j}, g_3). \quad \dots (a6')$$

この場合、復号処理部 5 4 は、自装置 5 0 の公開鍵 $p k_j$ を用いて検証を行う。

また、式 (a 6) の 7 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(g_3, g_1)^{x_j}.$$

また、式 (a 6) の 7 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4).$$

この場合、復号処理部 5 4 は、自装置 5 0 の公開鍵 $p k_j$ を用いて検証を行う。

[0258] 式 (a 6) の 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。

[0259] 検証が成功した場合 (又はステップ S T 5 1 の検証処理をスキップした場合)、復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と

一時データ記憶部52内の公開パラメータ $p a r$ 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43]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{z_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e\left(g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_j k}}, g^{z_j r k}\right) \cdot e\left(g^{\frac{x_j \delta_x}{h}}, g^{(L + w_i) r h}\right)}{e\left(g^{\frac{(\pi(x_j + \theta)/x_j) + (L + w_i) \delta_x}{s}}, g^{x_j r s}\right)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e\left(g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_j k}}, g^{\alpha z_j r k}\right) \cdot e\left(g^{\frac{\alpha y_j \delta_y}{h}}, g^{(L + w_i) r h}\right)}{e\left(g^{\frac{(\pi(\beta y_j + \theta)/y_j) + (L + w_i) \delta_y}{t}}, g^{\alpha y_j r t}\right)} \right)^{\frac{1}{z_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(x_j + \beta y_j + \theta)}, g^r) \cdot e(g^{x_j \delta_x}, g^{(L + w_i) r})}{e(g^{\pi(x_j + \theta) + (L + w_i) x_j \delta_x}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi(x_j + \beta y_j + \theta)}, g^{\alpha r}) \cdot e(g^{\alpha y_j \delta_y}, g^{(L + w_i) r})}{e(g^{\pi(\beta y_j + \theta) + (L + w_i) y_j \delta_y}, g^{\alpha r})} \right)^{\frac{1}{z_j}} \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0260] 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。

[0261] 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 、再暗号化鍵生成鍵 $r k_j$ 、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、ある期間において移譲元（図8の例では、グループ管理者）向けの暗号文についての復号権限を一度移譲先（図8の例では、例えばユーザA）

へ移譲した後でも、次の期間については当該移譲元向けの暗号文についての復号権限を当該移譲先に与えない、つまり、（当該移譲元向けの暗号文についての）当該移譲先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。

[0262] [変形例 8]

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。

[0263] 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'）。

[0264] 復号装置 50 は、公開パラメータ $p_a r$ と自装置 50 の秘密鍵 $s k_i$ を用いて、暗号化装置 20 において生成された暗号文データ C_i を次の検証式により検証する（ST51'）。

[数44]

$$\begin{aligned}
e(C_{2X}, u^{C_1} \cdot v) &= e(g, C_4)^{x_i}, \\
e(C_{2Y}, u^{C_1} \cdot v) &= e(g_1, C_4)^{y_i}, \\
e(C_{2Z}, u^{C_1} \cdot v) &= e(g, C_4)^{z_i}, \\
e(C_{2Z1}, u^{C_1} \cdot v) &= e(g_1, C_4)^{z_i}, \\
e(C_{2F}, u^{C_1} \cdot v) &= e(g, C_4)^{L+w_i}, \\
\hat{V}(C_1, \sigma, (L, C_3, C_4)) &= 1.
\end{aligned}$$

[0265] なお、復号装置50は、公開パラメータ $p a r$ と自装置50の公開鍵 $p k_i$ を用いて、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S T 4 1と同様に検証しても良い。

[0266] 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。

[0267] 検証が成功した場合（又はステップS T 5 1'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（S T 5 2'）。

[数45]

$$m = C_3 / e(g_4 g_5, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, C_{2X})^{\frac{1}{x_i}} \\ = m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g^{x_i r})^{\frac{1}{x_i}} \\ = m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g)^r = m. \end{aligned}$$

[0268] [変形例9]

変形例8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。

[0269] 暗号化装置20の暗号化パラメータ生成部23は、第1の実施形態のステップST21と同様に(s s k, s v k)を生成し(ST21')、暗号化データC₁に検証鍵s v kをセットする(C₁=s v k)。

[0270] 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, θ, δ_x, δ_y ∈ Z_p^{*}を生成して暗号文生成部24に送出する。

[0271] 暗号文生成部24は、これらの乱数r, s, t, k, h, θ, δ_x, δ_y、復号装置50の公開鍵p k_j、公開パラメータ、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 ∈ 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(ST22')。

[数46]

$$\begin{aligned}
C'_{2X} &= Y_{2j}^s, C''_{2X} = Y_{2j}^{rs}, C'_{2Y} = X_j^t, C''_{2Y} = X_j^{rt}, \\
C'_{2Z} &= Y_{2j}^k, C''_{2Z} = Y_{2j}^{rk}, C'_{2Z1} = X_j^k, C''_{2Z1} = X_j^{rk}, \\
C'_{2F} &= F_j(L)^h, C''_{2F} = F_j(L)^{rh}, \\
C_3 &= e(g_4 g_5, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r,
\end{aligned}$$

$$\begin{aligned}
C_{5X} &= (g_4 \cdot g_3^\theta \cdot F_j(L)^{\delta_y})^{\frac{1}{s}} = g^{\frac{\pi(\alpha+\theta)+(L+w_j)\delta_y}{s}}, \\
C_{5Y} &= (g_3^{1+\theta} \cdot F_j(L)^{\delta_x})^{\frac{1}{t}} = g^{\frac{\pi(1+\theta)+(L+w_j)\delta_x}{t}}, \\
C_{5Z} &= (g_4 \cdot g_3^{1+\theta})^{\frac{1}{k}} = g^{\frac{\pi(\alpha+1+\theta)}{k}}, \\
C_{5FX} &= (Y_{2j})^{\frac{\delta_y}{h}}, C_{5FY} = (X_j)^{\frac{\delta_x}{h}}
\end{aligned}$$

[0272] ステップS T 2 2' の終了後、暗号文生成部 2 4 は、ステップS T 2 3 と同様に、使い捨て署名 σ を生成する。

[0273] しかる後、暗号文生成部 2 4 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 $C_j = (L, C_1, C_{2X}', C_{2X}''', C_{2Y}', C_{2Y}''', C_{2Z}', C_{2Z}''', C_{2Z1}', C_{2Z1}''', C_{2F}', C_{2F}''', C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部 2 1 に書き込む。

[0274] 通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_j を復号装置 5 0 に送信する (S T 2 4')。

[0275] 復号装置 5 0 は、暗号化装置 2 0 において生成された暗号文データ C_j をステップS T 5 1 と同様に検証する (S T 5 1')。検証が成功した場合 (又はステップS T 5 1' の検証処理をスキップした場合)、復号装置 5 0 は、

秘密鍵 $s k_j$ と公開パラメータ $p a r$ 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（ST52'）。

[数47]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\frac{\pi(\alpha+1+\theta)}{k}}, g^{\beta y_j r k}) \cdot e(g^{\frac{\beta y_j \delta_y}{h}}, g^{(L+w_j) r h})}{e(g^{\frac{\pi(\alpha+\theta)+(L+w_j)\delta_y}{s}}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\pi(\alpha+1+\theta)}{k}}, g^{x_j r k}) \cdot e(g^{\frac{x_j \delta_x}{h}}, g^{(L+w_j) r h})}{e(g^{\frac{\pi(1+\theta)+(L+w_j)\delta_x}{t}}, g^{x_j r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(\alpha+1+\theta)}, g^{\beta r}) \cdot e(g^{\beta \delta_y}, g^{(L+w_j) r})}{e(g^{\pi(\alpha+\theta)+(L+w_j)\delta_y}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{\pi(\alpha+1+\theta)}, g^r) \cdot e(g^{\delta_x}, g^{(L+w_j) r})}{e(g^{\pi(1+\theta)+(L+w_j)\delta_x}, g^r)} \right) \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0276] （第3の実施形態）

本実施形態では、第1の実施形態において、変形例2に示した暗号化機能を省略する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施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。

[0277] （1）鍵セットアップ処理

始めに、鍵生成装置10の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、公開パラメータ

[数48]

$$\text{par} = \{\lambda, p, G, G_T, g, g_1, g_2, g_3, g_4, u, v, \text{Sig}\}$$

[0278] を生成する、又は外部から入手する（ST1）。ここで、 $g_3 = g^\pi$ 、 $g_4 = g_1^\pi$ である。

[0279] 鍵生成部14は、再暗号化鍵生成装置30の識別情報を*i*としたとき、 Z_p^* の元 x_i 、 y_i 、 z_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $sk_i = (x_i, y_i, z_i)$ とする。そして、鍵生成部14は、この秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成装置30の公開鍵 $pk_i = (X_i, Y_{1i}, Z_i, Z_{1i})$ を生成する。ここで、

[数49]

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

[0280] である。

[0281] さらに、鍵生成部14は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = (X_{3i}, Y_{2i})$ を生成する（ST3）。ここで、

[数50]

$$X_{3i} = g_3^{x_i}, Y_{2i} = g_2^{y_i}$$

[0282] である。

[0283] また同様に、鍵生成部14は、復号装置50の識別情報を*j*としたとき、 Z_p^* の元 x_j 、 y_j 、 z_j を Z_p^* からランダムに選択し、復号装置50の秘密鍵 $sk_j = (x_j, y_j, z_j)$ とする。そして、鍵生成部14は、この秘密鍵 sk_j と公開パラメータ par を用いて復号装置50の公開鍵 $pk_j = (X_j, Y_{1j}, Z_j, Z_{1j})$ を生成する。ここで、

[数51]

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

[0284] である。

[0285] さらに、鍵生成部 14 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = (X_{3j}, Y_{2j})$ を生成する (S T 6)。ここで、

[数52]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

[0286] である。

[0287] (2) 暗号化処理

第 1 の実施形態のステップ S T 2 1 と同様に、暗号化装置 20 の暗号化パラメータ生成部 23 は、 $(s s k, s v k)$ を生成し (S T 2 1)、暗号化データ C_1 に検証鍵 $s v k$ をセットする ($C_1 = s v k$)。

[0288] 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。

[0289] 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 $p k_i$ 、及び公開パラメータ $p a r$ 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_{2Y} , C_{2Z} , C_{2Z1} , C_3 , C_4 を生成する (S T 2 2)。

[数53]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_2, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

ステップ S T 2 2 の終了後、第 1 の実施形態のステップ S T 2 3 と同様に、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 $p a r$ における署名生成機能

$\hat{S}$ とステップ S T 2 1 で生成した署名鍵 $s s k$ により、使い捨て署名 σ を生成する (S T 2 3)。

[0290] 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

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。

[0291] 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 (ST24)。

[0292] (3) 再暗号化鍵生成処理

今、復号装置 50 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 30 (図 8 の例では、グループ管理者)宛の暗号文を、復号装置 50 (図 8 の例では、例えばユーザ A)宛の暗号文に再暗号化すること (つまり、暗号文の復号権限のユーザ A へ移譲すること) を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、復号装置 50 の再暗号化鍵生成鍵 rk_j を送信する。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、復号装置 50 の再暗号化鍵生成鍵 rk_j を取得して一時データ記憶部 32 に書き込む (ST31)。

[0293] 乱数生成部 36 は、乱数 $\theta \in Z_p^*$ を生成して再暗号化鍵生成部 34 に送出する。

[0294] 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 sk_i 、一時データ記憶部 32 内の復号装置 50 の再暗号化鍵生成鍵 rk_j 、及び公開パラメータ par を用いて、再暗号化鍵 R_{ij} を次式に示すように生成する (ST32)。

[0295] $R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$

ここで、

[数54]

$$R_{ij1} = (X_{3j} \cdot g^\theta)^{1/x_i} = g^{\frac{\pi x_j + \theta}{x_i}},$$

$$R_{ij2} = (Y_{2j} \cdot g^\theta)^{1/y_i} = g^{\frac{\beta y_j + \theta}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{2j} \cdot g^\theta)^{1/z_i} = g^{\frac{\pi x_j + \beta y_j + \theta}{z_i}}.$$

[0296] である。なお、上式では、 $g_2 = g^\beta$ と書き替えて表記している。

[0297] (4) 再暗号化処理

再暗号化装置40の再暗号化処理部44は、公開パラメータ p, a, r と再暗号化鍵生成装置30の公開鍵 p, k_i を用い、一時データ記憶部42内の暗号文データ C_i を次の検証式により検証する (ST41)。

[数55]

$$e(C_{2X}, u^{C_1} \cdot v) = e(X_i, C_4),$$

$$e(C_{2Y}, u^{C_1} \cdot v) = e(Y_{1i}, C_4),$$

$$e(C_{2Z}, u^{C_1} \cdot v) = e(Z_i, C_4),$$

$$e(C_{2Z1}, u^{C_1} \cdot v) = e(Z_{1i}, C_4),$$

$$\hat{V}(C_1, \sigma, (C_3, C_4)) = 1.$$

[0298] 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。

[0299] 検証が成功した場合（又はステップST41の検証処理をスキップした場合）、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。

[0300] 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に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ij} 、再暗号化鍵生成装置30の公開鍵 pk_i 、及び公開パラメータ par 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_{5X} , C_{5Y} , C_{5Z} を生成する (ST42)。

[数56]

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

[0301] ステップST42の終了後、再暗号化処理部44は、上記全ての再暗号化データ $C_{2X}' \sim C_{5Z}$ 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 $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ 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。

[0302] 通信部43は、制御部46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)。

[0303] (5) 復号処理

復号装置50の復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 sk_j と一時データ記憶部52内の公開パラメータ par を用い、一時データ記憶部52内の再暗号文データ C_j を次の検証式により検証する (ST51)。

[数57]

$$\begin{aligned}
e(C''_{2X}, u^{C_1} \cdot v) &= e(C'_{2X}, C_4), \\
e(C''_{2Y}, u^{C_1} \cdot v) &= e(C'_{2Y}, C_4), \\
e(C''_{2Z}, u^{C_1} \cdot v) &= e(C'_{2Z}, C_4), \\
e(C''_{2Z1}, u^{C_1} \cdot v) &= e(C'_{2Z1}, C_4), \\
e(C_{5Z}, C'_{2Z}) &= e(C_{5X}, C'_{2X}) \cdot e(g_2, g)^{y_j}, \\
e(C_{5Z}, C'_{2Z1}) &= e(C_{5Y}, C'_{2Y}) \cdot e(g, g_4)^{x_j}, \\
\hat{V}(C_1, \sigma, (C_3, C_4)) &= 1. \quad \dots (b1)
\end{aligned}$$

ここで、式 (b 1) の 6 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z1}) = e(C_{5Y}, C'_{2Y}) \cdot e(X_j, g_4).$$

この場合、復号処理部 5 4 は、自装置 5 0 の公開鍵 $p k_j$ を用いて検証を行う。

[0304] 式 (b 1) の 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。

[0305] 検証が成功した場合（又はステップ S T 5 1 の検証処理をスキップした場合）、復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と一時データ記憶部 5 2 内の公開パラメータ $p a r$ 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 5 2)。

[数58]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{(\pi x_j + \beta y_j + \theta)/z_i k}, g^{z_i r k})}{e(g^{(\pi x_j + \theta)/x_i s}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(\pi x_j + \beta y_j + \theta)/z_i k}, g^{\alpha z_i r k})}{e(g^{(\beta y_j + \theta)/y_i t}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^r)}{e(g^{\pi x_j + \theta}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^{\alpha r})}{e(g^{\beta y_j + \theta}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0306] 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 及び再暗号化鍵生成鍵 $r k_j$ に基づいて生成する構成により、第1の実施形態の効果と同様の効果を得ることができる。

[0307] また、上述したように本実施形態によれば、第1の実施形態における g_5 を省略する構成により、第1の実施形態において示した実施形態に比べ、公開パラメータや公開鍵のデータサイズを削減することができる。また、本実施形態によれば、第1の実施形態において示した実施形態に比べ、鍵セットアップ処理に要する計算量を削減することができる。

[0308] [変形例10]

第3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3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。

[0309] 本変形例における暗号化処理と、第3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'）。

[0310] 復号装置50は、公開パラメータ $p a r$ と自装置50の秘密鍵 $s k_i$ を用いて、暗号化装置20において生成された暗号文データ C_i を次の検証式により検証する（ST51'）。

[数59]

$$\begin{aligned} e(C_{2X}, u^{C_1} \cdot v) &= e(g, C_4)^{x_i}, \\ e(C_{2Y}, u^{C_1} \cdot v) &= e(g_1, C_4)^{y_i}, \\ e(C_{2Z}, u^{C_1} \cdot v) &= e(g, C_4)^{z_i}, \\ e(C_{2Z1}, u^{C_1} \cdot v) &= e(g_1, C_4)^{z_i}, \\ \hat{V}(C_1, \sigma, (C_3, C_4)) &= 1. \end{aligned}$$

... (b2)

[0311] なお、復号装置50は、公開パラメータ $p a r$ と自装置50の公開鍵 $p k_i$ を用いて、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と同様に検証しても良い。

[0312] 式（b2）の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。

[0313] 検証が成功した場合（又はステップS T 5 1' の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（S T 5 2'）。

[数60]

$$m = C_3 / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g)^r = m. \end{aligned}$$

[0314] （第4の実施形態）

本実施形態では、第3の実施形態において再暗号化鍵をある期間毎に更新する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施形態又は第2の実施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。

[0315] （1）鍵セットアップ処理

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 $p a r$ を、第3の実施形態と同様に生成する、又は外部から入手する（S T 1）。鍵生成部14は、再暗号化鍵生成装置30の識別情報を i としたとき、 Z_p^* の元 x_i, y_i, z_i, w_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置30

の秘密鍵 $s k_i = (x_i, y_i, z_i, w_i)$ とする。そして、鍵生成部 14 は、この秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成装置 30 の公開鍵 $p k_i = (X_i, Y_{1i}, Z_i, Z_{1i}, W_i)$ を生成する。ここで、

[数61]

$$X_i = g^{x_i}, \quad Y_{1i} = g_1^{y_i}, \quad Z_i = g^{z_i}, \\ Z_{1i} = g_1^{z_i}, \quad W_i = g^{w_i}$$

[0316] である。さらに、鍵生成部 14 は、秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_i = (X_{3i}, Y_{2i})$ を生成する (ST3)。ここで、

[数62]

$$X_{3i} = g_3^{x_i}, \quad Y_{2i} = g_2^{y_i}$$

[0317] である。

[0318] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、 Z_p^* の元 x_j, y_j, z_j, w_j を Z_p^* からランダムに選択し、復号装置 50 の秘密鍵 $s k_j = (x_j, y_j, z_j, w_j)$ とする。そして、鍵生成部 14 は、この秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて復号装置 50 の公開鍵 $p k_j = (X_j, Y_{1j}, Z_j, Z_{1j}, W_j)$ を生成する。ここで、

[数63]

$$X_j = g^{x_j}, \quad Y_{1j} = g_1^{y_j}, \quad Z_j = g^{z_j}, \\ Z_{1j} = g_1^{z_j}, \quad W_j = g^{w_j}$$

[0319] である。

[0320] さらに、鍵生成部 14 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = (X_{3j}, Y_{2j})$ を生成する (ST6)。ここで、

[数64]

$$X_{3j} = g_3^{x_j}, \quad Y_{2j} = g_2^{y_j}$$

[0321] である。

[0322] (2) 暗号化処理

第1の実施形態のステップST21と同様に、暗号化装置20の暗号化パラメータ生成部23は、 (ssk, svk) を生成し(ST21)、暗号化データ C_1 に検証鍵 svk をセットする($C_1 = svk$)。

[0323] 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。

[0324] 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 、公開パラメータ par 、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_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 , C_4 を生成する(ST22)。

[数65]

$$C_{2X} = X_i^r, \quad C_{2Y} = Y_{1i}^r, \quad C_{2Z} = Z_i^r, \quad C_{2Z1} = Z_{1i}^r, \\ C_{2F} = F_i(L)^r, \quad C_3 = e(g_1 g_2, g)^r \cdot m, \quad C_4 = (u^{svk} \cdot v)^r$$

ここで、関数 $F_i(L)$ は次式により定義される。

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

ステップST22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 par における署名生成機能 $\hat{S}$ とステップST21で生成した署名鍵 ssk による使い捨て署名 σ を次式に示すように生成する(ST23)。

$$\sigma = \hat{S}(ssk, (L, C_3, C_4))$$

[0325] 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 $C_i = (L, C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, \sigma)$ 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。

[0326] 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 (ST24)。

[0327] (3) 再暗号化鍵生成処理

今、復号装置 50 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 30 (図 8 の例では、グループ管理者) 宛の、時間パラメータの値として L を用いて生成された暗号文を、復号装置 50 (図 8 の例では、例えばユーザ A) 宛の暗号文に再暗号化すること (つまり、暗号文の復号権限のユーザ A へ移譲すること) を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、復号装置 50 の再暗号化鍵生成鍵 r_{kj} を送信する。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、復号装置 50 の再暗号化鍵生成鍵 r_{kj} を取得して一時データ記憶部 32 に書き込む (ST31)。

[0328] 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。

[0329] 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_{ki} 、一時データ記憶部 32 内の復号装置 50 の再暗号化鍵生成鍵 r_{kj} 、公開パラメータ p, a, r 、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)。

[0330] $R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$

ここで、

[数66]

$$\begin{aligned}
R_{ijL1} &= (X_{3j} \cdot g^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi x_j + \theta}{x_i} + (L+w_i)\delta_x}, \\
R_{ijL2} &= (Y_{2j} \cdot g^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\beta y_j + \theta}{y_i} + (L+w_i)\delta_y}, \\
R_{ijL3} &= (X_{3j} \cdot Y_{2j} \cdot g^\theta)^{1/z_i} = g^{\frac{\pi x_j + \beta y_j + \theta}{z_i}}, \\
R_{ijL4} &= g^{x_i \delta_x}, R_{ijL5} = g_1^{y_i \delta_y} = g^{\alpha y_i \delta_y}
\end{aligned}$$

[0331] 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。

[0332] (4) 再暗号化処理

再暗号化装置40の再暗号化処理部44は、公開パラメータ p, a, r 、一時データ記憶部42内の暗号文データ C_i に含まれている時間パラメータ L 、及び再暗号化鍵生成装置30の公開鍵 p, k_i を用い、一時データ記憶部42内の暗号文データ C_i を次の検証式により検証する（ST41）。

[数67]

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

[0333] 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。

[0334] 検証が成功した場合（又はステップS T 4 1の検証処理をスキップした場合）、再暗号化パラメータ生成部4 5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4 4に送出する。

[0335] 再暗号化処理部4 4は、これらの乱数 s, t, k, h 、一時データ記憶部4 2に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ijL} 、再暗号化鍵生成装置3 0の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ 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（S T 4 2）。

[数68]

$$\begin{aligned} C_{2X}' &= X_i^s, C_{2X}'' = C_{2X}^s = X_i^{rs}, C_{2Y}' = Y_{1i}^t, C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt}, \\ C_{2Z}' &= Z_i^k, C_{2Z}'' = C_{2Z}^k = Z_i^{rk}, C_{2Z1}' = Z_{1i}^k, C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk}, \\ C_{2F}' &= F_i(L)^h, C_{2F}'' = C_{2F}^h = F_i(L)^{rh}, \\ C_{5X} &= R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}}, \\ C_{5FX} &= R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}} \end{aligned}$$

[0336] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_{2X}' \sim C_{5FY}$ 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 $C_j = (L, C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部4 2に書き込む。

[0337] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する（S T 4 3）。

[0338] （5）復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘

密鍵 $s k_j$ と一時データ記憶部 52 内の公開パラメータ $p a r$ を用い、一時データ記憶部 52 内の再暗号文データ C_j を次の検証式により検証する (S T 51)。

[数69]

$$\begin{aligned}
 e(C''_{2X}, u^{C_1} \cdot v) &= e(C'_{2X}, C_4), \\
 e(C''_{2Y}, u^{C_1} \cdot v) &= e(C'_{2Y}, C_4), \\
 e(C''_{2Z}, u^{C_1} \cdot v) &= e(C'_{2Z}, C_4), \\
 e(C''_{2Z1}, u^{C_1} \cdot v) &= e(C'_{2Z1}, C_4), \\
 e(C''_{2F}, u^{C_1} \cdot v) &= e(C'_{2F}, C_4), \\
 e(C_{5Z}, C'_{2Z}) \cdot e(C_{5FX}, C'_{2F}) &= e(C_{5X}, C'_{2X}) \cdot e(g_2, g)^{y_j}, \\
 e(C_{5Z}, C'_{2Z1}) \cdot e(C_{5FY}, C'_{2F}) &= e(C_{5Y}, C'_{2Y}) \cdot e(g, g_4)^{x_j}, \\
 \hat{V}(C_1, \sigma, (L, C_3, C_4)) &= 1. \quad \dots (b3)
 \end{aligned}$$

ここで、式 (b3) の 7 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C'_{2Z1}) \cdot e(C_{5FY}, C'_{2F}) = e(C_{5Y}, C'_{2Y}) \cdot e(X_j, g_4).$$

この場合、復号処理部 54 は、自装置 50 の公開鍵 $p k_j$ を用いて検証を行う。

[0339] 式 (b3) の 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。

[0340] 検証が成功した場合 (又はステップ S T 51 の検証処理をスキップした場合)、復号処理部 54 は、秘密鍵記憶部 51 内の自装置 50 の秘密鍵 $s k_j$ と一時データ記憶部 52 内の公開パラメータ $p a r$ 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70]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e\left(g^{\frac{\pi x_j + \beta y_j + \theta}{z_i k}}, g^{z_i r k}\right) \cdot e\left(g^{\frac{x_i \delta_x}{h}}, g^{(L+w_i) r h}\right)}{e\left(g^{\frac{((\pi x_j + \theta)/x_i) + (L+w_i) \delta_x}{s}}, g^{x_i r s}\right)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e\left(g^{\frac{\pi x_j + \beta y_j + \theta}{z_i k}}, g^{\alpha z_i r k}\right) \cdot e\left(g^{\frac{\alpha y_i \delta_y}{h}}, g^{(L+w_i) r h}\right)}{e\left(g^{\frac{((\beta y_j + \theta)/y_i) + (L+w_i) \delta_y}{t}}, g^{\alpha y_i r t}\right)} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e\left(g^{\pi x_j + \beta y_j + \theta}, g^r\right) \cdot e\left(g^{x_i \delta_x}, g^{(L+w_i) r}\right)}{e\left(g^{\pi x_j + \theta + (L+w_i) x_i \delta_x}, g^r\right)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e\left(g^{\pi x_j + \beta y_j + \theta}, g^{\alpha r}\right) \cdot e\left(g^{\alpha y_i \delta_y}, g^{(L+w_i) r}\right)}{e\left(g^{\beta y_j + \theta + (L+w_i) y_i \delta_y}, g^{\alpha r}\right)} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0341] 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 、再暗号化鍵生成鍵 $r k_j$ 、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3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、ある期間において移譲元（図8の例では、グループ管理者）向けの暗号文についての復号権限を一度移譲先（図8の例では、例えばユーザA）へ移譲した後でも、次の期間については当該移譲元向けの暗号文についての復号権限を当該移譲先に与えない、つまり、（当該移譲元向けの暗号文についての）当該移譲先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。

[0342] また、上述したように本実施形態によれば、第2の実施形態における g_5 を

省略する構成により、第2の実施形態において示した実施形態に比べ、公開パラメータや公開鍵のデータサイズを削減することができる。また、本実施形態によれば、第2の実施形態において示した実施形態に比べ、鍵セットアップ処理に要する計算量を削減することができる。

[0343] [変形例11]

第4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4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。

[0344] 本変形例における暗号化処理と、第4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'）。

[0345] 復号装置50は、公開パラメータ $p_a r$ と自装置50の秘密鍵 $s k_i$ を用いて、暗号化装置20において生成された暗号文データ C_i を次の検証式により検証する（ST51'）。

[数71]

$$\begin{aligned}
 e(C_{2X}, u^{C_1} \cdot v) &= e(g, C_4)^{x_i}, \\
 e(C_{2Y}, u^{C_1} \cdot v) &= e(g_1, C_4)^{y_i}, \\
 e(C_{2Z}, u^{C_1} \cdot v) &= e(g, C_4)^{z_i}, \\
 e(C_{2Z1}, u^{C_1} \cdot v) &= e(g_1, C_4)^{z_i}, \\
 e(C_{2F}, u^{C_1} \cdot v) &= e(g, C_4)^{L+w_i}, \\
 \hat{V}(C_1, \sigma, (L, C_3, C_4)) &= 1.
 \end{aligned}$$

[0346] なお、復号装置50は、公開パラメータ $p a r$ と自装置50の公開鍵 $p k_i$ を用いて、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S T 4 1と同様に検証しても良い。

[0347] 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。

[0348] 検証が成功した場合（又はステップS T 5 1'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（S T 5 2'）。

[数72]

$$m = C_3 / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}} \\ = m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g^{x_i r})^{\frac{1}{x_i}} \\ = m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g)^r = m. \end{aligned}$$

[0349] (第5の実施形態)

本実施形態では、第1の実施形態において、サーバやユーザが正直なエンティティであり、複数のエンティティが結託する恐れのない場合の例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施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。

[0350] (1) 鍵セットアップ処理

始めに、鍵生成装置10の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、公開パラメータ

[数73]

$$\text{par} = \{\lambda, p, \mathbb{G}, \mathbb{G}_T, g, g_1, u, v, \text{Sig}\}$$

[0351] を生成する、又は外部から入手する(ST1)。

[0352] 鍵生成部14は、再暗号化鍵生成装置30の識別情報をiとしたとき、 Z_p^* の元 x_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置30の秘密鍵sk

$s_i = x_i$ とする。そして、鍵生成部14は、この秘密鍵 s_i と公開パラメータ p を用いて再暗号化鍵生成装置30の公開鍵 $p_k = X_i$ を生成する。ここで、

[数74]

$$X_i = g^{x_i}$$

[0353] である。

[0354] さらに、鍵生成部14は、秘密鍵 s_i と公開パラメータ p を用いて再暗号化鍵生成鍵 $r_k = X_{1i}$ を生成する（ST3）。ここで、

[数75]

$$X_{1i} = g_1^{x_i}$$

[0355] である。

[0356] また同様に、鍵生成部14は、復号装置50の識別情報を j としたとき、 Z_p^* の元 x_j を Z_p^* からランダムに選択し、復号装置50の秘密鍵 $s_j = x_j$ とする。そして、鍵生成部14は、この秘密鍵 s_j と公開パラメータ p を用いて復号装置50の公開鍵 $p_k = X_j$ を生成する。ここで、

[数76]

$$X_j = g^{x_j}$$

[0357] である。さらに、鍵生成部14は、秘密鍵 s_j と公開パラメータ p を用いて再暗号化鍵生成鍵 $r_k = X_{1j}$ を生成する（ST6）。ここで、

[数77]

$$X_{1j} = g_1^{x_j}$$

[0358] である。

[0359] (2) 暗号化処理

第1の実施形態のステップST21と同様に、暗号化装置20の暗号化パラメータ生成部23は、 $(s s k, s v k)$ 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($C_1 = s v k$)。

[0360] 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。

[0361] 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 $p k_i$ 、及び公開パラメータ $p a r$ 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_2, C_3, C_4 を生成する(ST22)。

[数78]

$$C_2 = X_i^r, C_3 = e(g_1, g)^r \cdot m, C_4 = (u^{s v k} \cdot v)^r$$

ステップST22の終了後、第1の実施形態のステップST23と同様に、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 $p a r$ における署名生成機能

$\hat{S}$ とステップST21で生成した署名鍵 $s s k$ により、使い捨て署名 σ を生成する(ST23)。

[0362] 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 $C_i = (C_1, C_2, C_3, C_4, \sigma)$ 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。

[0363] 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(ST24)。

[0364] (3) 再暗号化鍵生成処理

今、復号装置50(図8の例では、例えばユーザA)が、再暗号化鍵生成装置30(図8の例では、グループ管理者)宛の暗号文を、復号装置50(図8の例では、例えばユーザA)宛の暗号文に再暗号化すること(つまり、暗号文の復号権限のユーザAへ移譲すること)を承諾したとする。復号装置50は、再暗号化鍵生成装置30に、復号装置50の再暗号化鍵生成鍵 $r k_j$

を送信する。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、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部 32 に書き込む (S T 31)。

[0365] 本実施形態の再暗号化鍵の生成においては、乱数を生成する必要がないため、再暗号化鍵生成装置 30 の乱数生成部 36 は不要となる。

[0366] 再暗号化鍵生成部 34 は、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 の再暗号化鍵生成鍵 $r k_j$ 、及び公開パラメータ $p a r$ を用いて、再暗号化鍵 R_{ij} を次式に示すように生成する (S T 32)。

[数79]

$$R_{ij} = X_{1j}^{1/x_i} = g_1^{\frac{x_j}{x_i}}$$

[0367] (4) 再暗号化处理

再暗号化装置 40 の再暗号化处理部 44 は、公開パラメータ $p a r$ と再暗号化鍵生成装置 30 の公開鍵 $p k_i$ を用い、一時データ記憶部 42 内の暗号文データ C_i を次の検証式により検証する (S T 41)。

[数80]

$$e(C_2, u^{C_1} \cdot v) = e(X_i, C_4)$$

$$\hat{V}(C_1, \sigma, (C_3, C_4)) = 1.$$

[0368] ここで、上記 2 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。

[0369] 検証が成功した場合 (又はステップ S T 41 の検証処理をスキップした場合)、再暗号化パラメータ生成部 45 は、乱数 $t \in \mathbb{Z}_p^*$ を生成して再暗号化处理部 44 に送出する。

[0370] 再暗号化处理部 44 は、この乱数 t 、一時データ記憶部 42 に記憶されて

いる、暗号文データ C_i 、再暗号化鍵 R_{ij} 、再暗号化鍵生成装置 30 の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ を用いて、次式に示すように、再暗号化データ C_2' 、 C_2'' 、 C_2''' を生成する (S T 4 2)。

[数81]

$$C_2' = X_i^t, C_2'' = R_{ij}^{1/t} = g_1^{\frac{x_j}{tx_i}}, C_2''' = C_2^t = X_i^{rt}$$

[0371] ステップ S T 4 2 の終了後、再暗号化処理部 44 は、上記全ての再暗号化データ $C_2' \sim C_2'''$ を、暗号文データ C_i 内の暗号化データ C_2 と置換して再暗号文データ $C_j = (C_1, C_2', C_2'', C_2''', C_3, C_4, \sigma)$ 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。

[0372] 通信部 43 は、制御部 46 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 (S T 4 3)。

[0373] (5) 復号処理

復号装置 50 の復号処理部 54 は、秘密鍵記憶部 51 内の自装置 50 の秘密鍵 $s k_j$ と一時データ記憶部 52 内の公開パラメータ $p a r$ を用い、一時データ記憶部 52 内の再暗号文データ C_j を次の検証式により検証する (S T 5 1)。

[数82]

$$\begin{aligned} e(C_2', C_2'') &= e(g, g_1)^{x_j}, \\ e(C_2''', u^{C_1} \cdot v) &= e(C_2', C_4), \\ \hat{V}(C_1, \sigma, (C_3, C_4)) &= 1. \end{aligned} \quad \dots (c 1)$$

ここで、式 (c 1) の 1 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_2', C_2'') = e(X_j, g_1)$$

この場合、復号処理部 54 は、自装置 50 の公開鍵 $p k_j$ を用いて検証を行う。

[0374] 式(c1)の3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。

[0375] 検証が成功した場合（又はステップST51の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 $s k_j$ と一時データ記憶部52内の公開パラメータ $p a r$ 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83]

$$m = C_3 / e(C_2'', C_2''')^{1/x_j}$$

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。

$$\begin{aligned} C_3 / e(C_2'', C_2''')^{1/x_j} &= C_3 / e(g_1^{\frac{x_j}{tx_i}}, g^{x_i r t})^{1/x_j} \\ &= m \cdot e(g_1, g)^r / e(g_1^{x_j}, g^r)^{1/x_j} = m. \end{aligned}$$

[0376] 上述したように本実施形態によれば、再暗号化鍵 R_{ij} を再暗号化鍵生成鍵 $r k_j$ に基づいて生成する構成により、移譲先（図8の例では、例えばユーザA）が再暗号化鍵生成鍵を移譲元（図8の例では、グループ管理者）に通知しなければ再暗号化鍵が生成され得ないため、移譲先の承諾なく再暗号化（つまり、暗号文の復号権限の当該移譲先への移譲）を行わないようにすることができる。

[0377] また、上述したように本実施形態によれば、第1の実施形態における $g_2 \sim g_5$ を省略する構成により、第1の実施形態において示した実施形態に比べ、公開パラメータ、公開鍵、再暗号化鍵生成鍵、再暗号化鍵、秘密鍵、暗号文データ、及び再暗号文データのデータサイズを削減することができる。また、本実施形態によれば、第1の実施形態において示した実施形態に比べ、鍵セットアップ処理、暗号化処理、再暗号化鍵生成処理、再暗号化処理、及び復号処理に要する計算量を削減することができる。

[0378] [変形例 1 2]

第 5 の実施形態では、暗号化装置 2 0 において暗号文データを生成し、再暗号化装置 4 0 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 5 0 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 5 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。

[0379] 本変形例における暗号化処理と、第 5 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 5 0 の識別情報を i とする。この場合、暗号化装置 2 0 の通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_i を復号装置 5 0 に送信する (ST 2 4')。

[0380] 復号装置 5 0 は、公開パラメータ $p a r$ と自装置 5 0 の秘密鍵 $s k_i$ を用いて、暗号化装置 2 0 において生成された暗号文データ C_i を次の検証式により検証する (ST 5 1')。

[数 84]

$$e\left(C_2, u^{C_1} \cdot v\right) = e(g, C_4)^{x_i}$$

$$\hat{V}(C_1, \sigma, (C_3, C_4)) = 1. \quad \dots (c 2)$$

[0381] なお、復号装置 5 0 は、公開パラメータ $p a r$ と自装置 5 0 の公開鍵 $p k_i$ を用いて、暗号化装置 2 0 において生成された暗号文データ C_i をステップ S T 4 1 と同様に検証しても良い。

[0382] 式 (c 2) の 2 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。

[0383] 検証が成功した場合 (又はステップ S T 5 1' の検証処理をスキップした

場合)、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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 (S T 5 2')。

[数85]

$$m = C_3 / e(C_2, g_1)^{1/x_i}$$

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。

$$\begin{aligned} C_3 / e(g_1, C_2)^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^r / e(g_1, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^r / e(g_1, g)^r = m. \end{aligned}$$

[0384] [変形例13]

変形例12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5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。

[0385] 暗号化装置20の暗号化パラメータ生成部23は、第1の実施形態のステップS T 2 1と同様に ($s s k, s v k$) を生成し (S T 2 1')、暗号化データ C_1 に検証鍵 $s v k$ をセットする ($C_1 = s v k$)。

[0386] また、暗号化パラメータ生成部23は、2つの乱数 $r, t \in \mathbb{Z}_p^*$ を生成して暗号文生成部24に送出する。

[0387] 暗号文生成部24は、これらの乱数 r 、 t 、復号装置50の公開鍵 $p k_j$ 、及び公開パラメータを用いて、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_2' 、 C_2'' 、 C_2''' 、 C_3 、 C_4 を生成する（ST22'）。

[数86]

$$C_2' = X_j^t, C_2'' = g_1^{1/t}, C_2''' = X_j^{rt},$$

$$C_3 = e(g_1, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

[0388] 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（ST23'）。

[0389] 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 $C_j = (C_1, C_2', C_2'', C_2''', C_3, C_4, \sigma)$ 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。

[0390] 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（ST24'）。

[0391] 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 を第5の実施形態のステップST51と同様に検証する（ST51'）。

[0392] 検証が成功した場合（又はステップST51'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_j$ と公開パラメータ $p a r$ 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（ST52'）。

[数87]

$$m = C_3 / e(C_2'', C_2''')^{1/x_j}$$

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。

$$\begin{aligned} C_3 / e(C_2'', C_2''')^{1/x_j} &= C_3 / e(g_1^{1/t}, g^{x_j r t})^{1/x_j} \\ &= m \cdot e(g_1, g)^r / e(g_1, g^r) = m. \end{aligned}$$

[0393] (第6の実施形態)

本実施形態では、第5の実施形態において再暗号化鍵をある期間毎に更新する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施形態又は第2の実施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。

[0394] (1) 鍵セットアップ処理

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 a rを、第5の実施形態と同様に生成する、又は外部から入手する(ST1)。鍵生成部14は、再暗号化鍵生成装置30の識別情報をiとしたとき、 Z_p^* の元 x_i, y_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $s k_i = (x_i, y_i)$ とする。そして、鍵生成部14は、この秘密鍵 $s k_i$ と公開パラメータp a rを用いて再暗号化鍵生成装置30の公開鍵 $p k_i = (X_i, Y_i)$ を生成する。ここで、

[数88]

$$X_i = g^{x_i}, Y_i = g^{y_i}$$

[0395] である。

[0396] さらに、鍵生成部14は、秘密鍵 $s k_i$ と公開パラメータp a rを用いて再

暗号化鍵生成鍵 $r k_i = X_{1i}$ を生成する (S T 3)。ここで、

[数89]

$$X_{1i} = g_1^{x_i}$$

[0397] である。

[0398] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、 Z_p^* の元 x_j, y_j を Z_p^* からランダムに選択し、復号装置 50 の秘密鍵 $s k_j = (x_j, y_j)$ とする。そして、鍵生成部 14 は、この秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて復号装置 50 の公開鍵 $p k_j = (X_j, Y_j)$ を生成する。ここで、

[数90]

$$X_j = g^{x_j}, Y_j = g^{y_j}$$

[0399] である。

[0400] さらに、鍵生成部 14 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = X_{1j}$ を生成する (S T 6)。ここで、

[数91]

$$X_{1j} = g_1^{x_j}$$

[0401] である。

[0402] (2) 暗号化処理

第 1 の実施形態のステップ S T 2 1 と同様に、暗号化装置 20 の暗号化パラメータ生成部 23 は、 $(s s k, s v k)$ を生成し (S T 2 1)、暗号化データ C_0 に検証鍵 $s v k$ をセットする ($C_0 = s v k$)。

[0403] また、暗号化パラメータ生成部 23 は、乱数 $s \in Z_p^*$ を生成して暗号文生成部 24 に送出する。

[0404] 暗号文生成部 24 は、この乱数 s 、再暗号化鍵生成装置 30 の公開鍵 $p k_j$

、公開パラメータ $p a r$ 、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_1, C_2, C_3, C_4 を生成する (S T 2 2)。

[数92]

$$C_1 = X_i^s, C_2 = F_i(L)^s,$$

$$C_3 = e(g_1, g)^s \cdot m, C_4 = (u^{svk} \cdot v)^s$$

ここで、関数 $F_i(L)$ は次式により定義される。

$$F_i(L) = g^L \cdot Y_i = g^{L+y_i} \quad (L \in \mathbb{Z}_p^*)$$

ステップ S T 2 2 の終了後、暗号文生成部 2 4 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 $p a r$ における署名生成機能 $\hat{S}$ とステップ S T 2 1 で生成した署名鍵 $s s k$ 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 2 3)。

$$\sigma = \hat{S}(ssk, (L, C_3, C_4))$$

[0405] しかる後、暗号文生成部 2 4 は、時間パラメータ L 、上記全ての暗号化データ $C_0 \sim C_4$ 、及び使い捨て署名 σ を含む暗号文データ $C_i = (L, C_0, C_1, C_2, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部 2 1 に書き込む。

[0406] 通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_i を再暗号化装置 4 0 に送信する (S T 2 4)。

[0407] (3) 再暗号化鍵生成処理

今、復号装置 5 0 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 3 0 (図 8 の例では、グループ管理者) 宛の、時間パラメータの値として L を用いて生成された暗号文を、復号装置 5 0 (図 8 の例では、例えばユーザ A) 宛の暗号文に再暗号化すること (つまり、暗号文の復号権限のユーザ A へ移譲すること) を承諾したとする。復号装置 5 0 は、再暗号化鍵生成装置 3 0 に、復号装置 5 0 の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部 32 に書き込む（S T 31）。

[0408] 乱数生成部 36 は、乱数 $r \in Z_p^*$ を生成して再暗号化鍵生成部 34 に送出する。

[0409] 再暗号化鍵生成部 34 は、この乱数 r 、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 の再暗号化鍵生成鍵 $r k_j$ 、公開パラメータ $p a r$ 、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（S T 32）。

[0410] $R_{ijL} = (A_{ijL}, B_{ijL})$

ここで、

[数93]

$$A_{ijL} = X_{1j}^{1/x_i} \cdot (g^{L+y_i})^r, \quad B_{ijL} = g^{x_i r}$$

[0411] である。

[0412] (4) 再暗号化处理

再暗号化装置 40 の再暗号化处理部 44 は、公開パラメータ $p a r$ 、一時データ記憶部 42 内の暗号文データ C_i に含まれている時間パラメータ L 、及び再暗号化鍵生成装置 30 の公開鍵 $p k_i$ を用い、一時データ記憶部 42 内の暗号文データ C_i を次の検証式により検証する（S T 41）。

[数94]

$$\begin{aligned} e(X_i, C_4) &= e(C_1, u^{C_0} \cdot v), \\ e(X_i, C_2) &= e(C_1, F_i(L)), \\ \hat{V}(C_0, \sigma, (L, C_3, C_4)) &= 1. \end{aligned}$$

[0413] ここで、上記 3 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。

[0414] 検証が成功した場合（又はステップS T 4 1の検証処理をスキップした場合）、再暗号化パラメータ生成部4 5は、2つの乱数 $t_1, t_2 \in Z_p^*$ を生成して再暗号化処理部4 4に送出する。

[0415] 再暗号化処理部4 4は、これらの乱数 t_1, t_2 、一時データ記憶部4 2に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ijL} 、再暗号化鍵生成装置3 0の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ を用いて、次式に示すように、再暗号化データ $C_1', C_1'', C_1''', C_2', C_2'', C_2'''$ を生成する（S T 4 2）。

[数95]

$$C_1' = X_i^{t_1}, C_1'' = (A_{ijL})^{1/t_1}, C_1''' = C_1^{t_1} = X_i^{st_1}, \\ C_2' = F_i(L)^{t_2}, C_2'' = B_{ijL}^{1/t_2}, C_2''' = C_2^{t_2} = F_i(L)^{st_2}$$

[0416] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_1' \sim C_2'''$ を、暗号文データ C_i 内の暗号化データ C_1, C_2 と置換して再暗号文データ $C_j = (L, C_0, C_1', C_1'', C_1''', C_2', C_2'', C_2''', C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部4 2に書き込む。

[0417] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する（S T 4 3）。

[0418] （5）復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ と一時データ記憶部5 2内の公開パラメータ $p a r$ を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する（S T 5 1）。

[数96]

$$\begin{aligned}
e(C_1''', u^{C_0} \cdot v) &= e(C_1', C_4), \\
e(C_2''', u^{C_0} \cdot v) &= e(C_2', C_4), \\
e(C_1', C_1'') &= e(g, g_1)^{x_j} \cdot e(C_2', C_2''), \\
\hat{V}(C_0, \sigma, (L, C_3, C_4)) &= 1.
\end{aligned}
\quad \dots (c3)$$

ここで、式(c3)の3番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_1', C_1'') = e(X_j, g_1) \cdot e(C_2', C_2'')$$

この場合、復号処理部54は、自装置50の公開鍵 pk_j を用いて検証を行う。

[0419] 式(c3)の4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。

[0420] 検証が成功した場合（又はステップST51の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 sk_j と一時データ記憶部52内の公開パラメータ par 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97]

$$m = C_3 \cdot (e(C_2'', C_2''') / e(C_1'', C_1'''))^{1/x_j}.$$

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。

$$\begin{aligned}
& C_3 \cdot \{e(g^{x_i r/t_2}, F_i(L)^{st_2}) / e((g_1^{x_j/x_i} \cdot F_i(L)^r)^{1/t_1}, g^{sx_i t_1})\}^{1/x_j} \\
&= C_3 \cdot \{e(g^{x_i r}, F_i(L)^s) / e(g_1^{x_j/x_i} \cdot F_i(L)^r, g^{sx_i})\}^{1/x_j} \\
&= C_3 \cdot \{e(g^{x_i r}, F_i(L)^s) / e(g_1^{x_j} \cdot F_i(L)^{x_i r}, g^s)\}^{1/x_j} \\
&= m \cdot e(g_1, g)^s \cdot \{1/e(g_1^{x_j}, g^s)\}^{1/x_j} = m.
\end{aligned}$$

[0421] 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 r 、再暗号化鍵生成鍵 $r k_j$ 、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5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、ある期間において移譲元（図8の例では、グループ管理者）向けの暗号文についての復号権限を一度移譲先（図8の例では、例えばユーザA）へ移譲した後も、次の期間については当該移譲元向けの暗号文についての復号権限を当該移譲先に与えない、つまり、（当該移譲元向けの暗号文についての）当該移譲先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。

[0422] また、上述したように本実施形態によれば、第2の実施形態における $g_2 \sim g_5$ を省略する構成により、第2の実施形態において示した実施形態に比べ、公開パラメータ、公開鍵、再暗号化鍵生成鍵、再暗号化鍵、秘密鍵、暗号文データ、及び再暗号文データのデータサイズを削減することができる。また、本実施形態によれば、第2の実施形態において示した実施形態に比べ、鍵セットアップ処理、暗号化処理、再暗号化鍵生成処理、再暗号化処理、及び復号処理に要する計算量を削減することができる。

[0423] [変形例14]

第6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6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。

[0424] 本変形例における暗号化処理と、第6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 (ST 24')。

[0425] 復号装置 50 は、公開パラメータ $p a r$ と自装置 50 の秘密鍵 $s k_i$ を用いて、暗号化装置 20 において生成された暗号文データ C_i を次の検証式により検証する (ST 51')。

[数98]

$$\begin{aligned} e(g, C_4)^{x_i} &= e(C_1, u^{C_0} \cdot v), \\ e(g, C_2)^{x_i} &= e(C_1, g)^{L+y_i}, \\ \hat{V}(C_0, \sigma, (L, C_3, C_4)) &= 1. \end{aligned} \quad \dots (c 4)$$

[0426] なお、復号装置 50 は、公開パラメータ $p a r$ と自装置 50 の公開鍵 $p k_i$ を用いて、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 ST 41 と同様に検証しても良い。

[0427] 式 (c 4) の 3 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。

[0428] 検証が成功した場合 (又はステップ ST 51' の検証処理をスキップした場合)、復号装置 50 は、自装置 50 の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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 (ST 52')。

[数99]

$$m = C_3 / e(C_1, g_1)^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} & C_3 / e(C_1, g_1)^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^s / e(g^{x_i s}, g_1)^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^s / e(g, g_1)^s = m. \end{aligned}$$

[0429] [変形例 1 5]

変形例 1 4 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 6 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 5 0 の識別情報を j とする。

[0430] 暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、第 1 の実施形態のステップ S T 2 1 と同様に (s s k, s v k) を生成し (S T 2 1')、暗号化データ C₀ に検証鍵 s v k をセットする (C₀ = s v k)。

[0431] また、暗号化パラメータ生成部 2 3 は、2 つの乱数 t₁, t₂ ∈ Z_p^{*} を生成して暗号文生成部 2 4 に送出する。

[0432] 暗号文生成部 2 4 は、これらの乱数 t₁, t₂、復号装置 5 0 の公開鍵 p k_j、公開パラメータ、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 ∈ G_T に対して、以下の暗号化データ C₁', C₁'', C₁'', C₂' ,

C_2', C_2'', C_3, C_4 を生成する（ST 2 2'）。

[数100]

$$\begin{aligned} C_1' &= X_j^{t_1}, C_1'' = (F_j(L) \cdot g_1)^{1/t_1}, C_1''' = X_j^{st_1}, \\ C_2' &= F_j(L)^{t_2}, C_2'' = X_j^{1/t_2}, C_2''' = F_j(L)^{st_2}, \\ C_3 &= e(g_1, g)^s \cdot m, C_4 = (u^{svk} \cdot v)^s \end{aligned}$$

[0433] ステップST 2 2'の終了後、暗号文生成部24は、ステップST 2 3と同様に、使い捨て署名 σ を生成する。

[0434] 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 $C_0 \sim C_4$ と使い捨て署名 σ とを含む暗号文データ $C_j = (L, C_0, C_1', C_1'', C_1''', C_2', C_2'', C_2''', C_3, C_4, \sigma)$ 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。

[0435] 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（ST 2 4'）。

[0436] 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ST 5 1と同様に検証する（ST 5 1'）。検証が成功した場合（又はステップST 5 1'の検証処理をスキップした場合）、復号装置50は、秘密鍵 s_{k_j} と公開パラメータ $p_a r$ 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（ST 5 2'）。

[数101]

$$m = C_3 \cdot (e(C_2'', C_2''')/e(C_1'', C_1'''))^{1/x_j}.$$

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。

$$\begin{aligned} & C_3 \cdot \{e(C_2'', C_2''')/e(C_1'', C_1''')\}^{1/x_j} \\ &= C_3 \cdot \{e(g^{x_j/t_2}, F_j(L)^{st_2})/e((F_j(L) \cdot g_1)^{1/t_1}, g^{sx_j t_1})\}^{1/x_j} \\ &= C_3 \cdot \{e(g^{x_j}, F_j(L)^s)/e(F_j(L) \cdot g_1, g^{sx_j})\}^{1/x_j} \\ &= m \cdot e(g_1, g)^s \cdot \{1/e(g_1, g^{sx_j})\}^{1/x_j} = m. \end{aligned}$$

[0437] (第7の実施形態)

本実施形態では、第1の実施形態において使い捨て署名を省略する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施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。

[0438] (1) 鍵セットアップ処理

始めに、鍵生成装置10の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、公開パラメータ

[数102]

$$\text{par} = \{\lambda, p, \mathbb{G}, \mathbb{G}_T, g, g_1, g_2, g_3, g_4, g_5, u, v, H\}$$

[0439] を生成する、又は外部から入手する(ST1)。ここで、 $g_3 = g^\pi$ 、 $g_4 = g_1^\pi$ 、 $g_5 = g_2^\pi$ である。また、Hは次式により定義されるハッシュ関数である。

[数103]

$$H : \mathbb{G}^4 \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$$

[0440] 鍵生成部14は、再暗号化鍵生成装置30の識別情報を*i*としたとき、 $\mathbb{Z}_p^*$ の元 x_i, y_i, z_i を $\mathbb{Z}_p^*$ からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $sk_i = (x_i, y_i, z_i)$ とする。そして、鍵生成部14は、この秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成装置30の公開鍵 $pk_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i})$ を生成する。ここで、

[数104]

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

[0441] である。なお、後述する式(d3)を用いた検証処理を行わない場合には、データ Y_{2i} を省略してもよい。すなわち、公開鍵 pk_i は、データ X_i, Y_{1i}, Z_i, Z_{1i} を含んでいればよい。

[0442] さらに、鍵生成部14は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = (X_{3i}, Y_{5i})$ を生成する(ST3)。ここで、

[数105]

$$X_{3i} = g_3^{x_i}, Y_{5i} = g_5^{y_i}$$

[0443] である。

[0444] また同様に、鍵生成部14は、復号装置50の識別情報を*j*としたとき、 $\mathbb{Z}_p^*$ の元 x_j, y_j, z_j を $\mathbb{Z}_p^*$ からランダムに選択し、復号装置50の秘密鍵 $sk_j = (x_j, y_j, z_j)$ とする。そして、鍵生成部14は、この秘密鍵 sk_j と公開パラメータ par を用いて復号装置50の公開鍵 $pk_j = (X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j})$ を生成する。ここで、

[数106]

$$X_j = g^{X_j}, \quad Y_{1j} = g_1^{Y_j}, \quad Y_{2j} = g_2^{Y_j}, \\ Z_j = g^{Z_j}, \quad Z_{1j} = g_1^{Z_j}$$

[0445] である。前述同様に、後述する式 (d 3) を用いた検証処理を行わない場合には、データ Y_{2j} を省略してもよい。すなわち、公開鍵 $p k_j$ は、データ X_j , Y_{1j} , Z_j , Z_{1j} を含んでいけばよい。

[0446] さらに、鍵生成部 1 4 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = (X_{3j}, Y_{5j})$ を生成する (S T 6)。ここで、

[数107]

$$X_{3j} = g_3^{X_j}, \quad Y_{5j} = g_5^{Y_j}$$

[0447] である。

[0448] (2) 暗号化処理

本実施形態においては、使い捨て署名を用いないため、第 1 の実施形態のステップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。

[0449] 暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、乱数 $r \in Z_p^*$ を生成して暗号文生成部 2 4 に送出する。

[0450] 暗号文生成部 2 4 は、この乱数 r 、再暗号化鍵生成装置 3 0 の公開鍵 $p k_j$ 、及び公開パラメータ $p a r$ 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_{2Y} , C_{2Z} , C_{2Z1} , C_3 , C_4 を生成する (S T 2 2)。

[数108]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_3 = e(g_4 g_5, g)^r \cdot m,$$

$$C_4 = (u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v)^r$$

[0451] ステップS T 2 2の終了後、暗号文生成部2 4は、上記全ての暗号化データ $C_{2X} \sim C_4$ を含む暗号文データ $C_i = (C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4)$ を生成し、得られた暗号文データを一時データ記憶部2 1に書き込む。

[0452] 通信部2 2は、制御部2 5に制御されて一時データ記憶部2 1内の暗号文データ C_i を再暗号化装置4 0に送信する(S T 2 4)。

[0453] (3) 再暗号化鍵生成処理

今、復号装置5 0(図8の例では、例えばユーザA)が、再暗号化鍵生成装置3 0(図8の例では、グループ管理者)宛の暗号文を、復号装置5 0(図8の例では、例えばユーザA)宛の暗号文に再暗号化すること(つまり、暗号文の復号権限のユーザAへ移譲すること)を承諾したとする。復号装置5 0は、再暗号化鍵生成装置3 0に、復号装置5 0の再暗号化鍵生成鍵 $r k_j$ を送信する。再暗号化鍵生成装置3 0の通信部3 3は、制御部3 5に制御されて、復号装置5 0の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部3 2に書き込む(S T 3 1)。

[0454] 乱数生成部3 6は、乱数 $\theta \in Z_p^*$ を生成して再暗号化鍵生成部3 4に送出する。

[0455] 再暗号化鍵生成部3 4は、この乱数 θ 、秘密鍵記憶部3 1内の再暗号化鍵生成装置3 0の秘密鍵 $s k_i$ 、一時データ記憶部3 2内の復号装置5 0の再暗号化鍵生成鍵 $r k_j$ 、及び公開パラメータ $p a r$ を用いて、再暗号化鍵 R_{ij} を次式に示すように生成する(S T 3 2)。

[0456] $R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$

ここで、

[数109]

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}.$$

[0457] である。なお、上式では、 $g_2 = g^\beta$ と書き替えて表記している。

[0458] (4) 再暗号化处理

再暗号化装置40の再暗号化处理部44は、公開パラメータ p, a, r と再暗号化鍵生成装置30の公開鍵 p, k_i を用い、一時データ記憶部42内の暗号文データ C_i を次の検証式により検証する(ST41)。

[数110]

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

[0459] ここで、上記4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。

[0460] 検証が成功した場合（又はステップST41の検証処理をスキップした場合）、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 4 4 に送出する。

[0461] 再暗号化処理部 4 4 は、これらの乱数 s , t , k 、一時データ記憶部 4 2 に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ij} 、再暗号化鍵生成装置 3 0 の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ 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_{5X} , C_{5Y} , C_{5Z} を生成する (S T 4 2)。

[数111]

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

[0462] ステップ S T 4 2 の終了後、再暗号化処理部 4 4 は、上記全ての再暗号化データ $C_{2X}' \sim C_{5Z}$ と再暗号化鍵生成装置 3 0 の識別情報 i を、暗号文データ C_i に付加して再暗号文データ $C_j = (C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, i)$ 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 4 2 に書き込む。

[0463] 通信部 4 3 は、制御部 4 6 に制御されて一時データ記憶部 4 2 内の再暗号文データ C_j を復号装置 5 0 に送信する (S T 4 3)。

[0464] (5) 復号処理

復号装置 5 0 の復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ 、一時データ記憶部 5 2 内の公開パラメータ $p a r$ 、及び一時データ記憶部 5 2 内の再暗号文データ C_j に含まれている再暗号化鍵生成装置 3 0 の識別情報 i により特定される再暗号化鍵生成装置 3 0 の公開鍵 $p k_i$ を用い、一時データ記憶部 5 2 内の再暗号文データ C_j を次の検証式により検証する (S T 5 1)。

[数112]

$$\begin{aligned}
e(C_{2X}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2X}', C_4), \\
e(C_{2Y}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2Y}', C_4), \\
e(C_{2Z}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2Z}', C_4), \\
e(C_{2Z1}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2Z1}', C_4), \\
e(C_{5Z}, C_{2Z}') &= e(C_{5X}, C_{2X}') \cdot e(g_2, g_3)^{y_j}, \\
e(C_{5Z}, C_{2Z1}') &= e(C_{5Y}, C_{2Y}') \cdot e(g, g_4)^{x_j}, \\
e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(X_i, C_4), \\
e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Y_{1i}, C_4), \\
e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Z_i, C_4), \\
e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Z_{1i}, C_4). \dots (d1)
\end{aligned}$$

ここで、式 (d1) の5番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z}') = e(C_{5X}, C_{2X}') \cdot e(g_5, g)^{y_j}. \dots (d2)$$

また、式 (d1) の5番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z}') = e(C_{5X}, C_{2X}') \cdot e(Y_{2j}, g_3). \dots (d3)$$

この場合、復号処理部54は、自装置50の公開鍵 pk_j を用いて検証を行う。

また、式 (d1) の6番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z1}') = e(C_{5Y}, C_{2Y}') \cdot e(g_3, g_1)^{x_j}. \dots (d4)$$

また、式 (d1) の6番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z1}') = e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4). \dots (d5)$$

この場合、復号処理部54は、自装置50の公開鍵 pk_j を用いて検証を行う。

[0465] 式 (d1) の10個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。

[0466] 検証が成功した場合（又はステップS T 5 1の検証処理をスキップした場合）、復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ と一時データ記憶部5 2内の公開パラメータ $p a r$ 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 5 2）。

[数113]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{(\pi x_j + \beta y_j + \theta)/z_i k}, g^{z_i r k})}{e(g^{(\pi x_j + \theta)/x_i s}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(\pi x_j + \beta y_j + \theta)/z_i k}, g^{\alpha z_i r k})}{e(g^{(\beta y_j + \theta)/y_i t}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^r)}{e(g^{\pi x_j + \theta}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^{\alpha r})}{e(g^{\beta y_j + \theta}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0467] 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 及び再暗号化鍵生成鍵 $r k_j$ に基づいて生成する構成により、第1の実施形態の効果と同様の効果を得ることができる。

[0468] また、上述したように本実施形態によれば、第1の実施形態における使い捨て署名 σ を省略する構成により、第1の実施形態において示した実施形態に比べ、暗号文データや再暗号文データのデータサイズを削減することがで

きる。また、本実施形態によれば、第 1 の実施形態において示した実施形態に比べ、暗号化処理や再暗号化処理に要する計算量を削減することができる。

[0469] [変形例 16]

第 7 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 7 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。

[0470] 本変形例における暗号化処理と、第 7 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')。

[0471] 復号装置 50 は、公開パラメータ p, r と自装置 50 の秘密鍵 s, k_i を用いて、暗号化装置 20 において生成された暗号文データ C_i を次の検証式により検証する (ST51')。

[数114]

$$\begin{aligned} e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g, C_4)^{x_i}, \\ e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g_1, C_4)^{y_i}, \\ e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g, C_4)^{z_i}, \\ e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g_1, C_4)^{z_i}. \end{aligned} \quad \dots (d6)$$

[0472] なお、復号装置 50 は、公開パラメータ $p a r$ と自装置 50 の公開鍵 $p k_i$ を用いて、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 S T 4 1 と同様に検証しても良い。

[0473] 式 (d 6) の 4 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。

[0474] 検証が成功した場合（又はステップ S T 5 1' の検証処理をスキップした場合）、復号装置 50 は、自装置 50 の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（S T 5 2' ）。

[数115]

$$m = C_3 / e(g_4 g_5, C_2 X)^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} & m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, C_2 X)^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g)^r = m. \end{aligned}$$

[0475] [変形例 1 7]

変形例 1 6 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 7 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。

[0476] 本変形例においても、使い捨て署名を用いないため、第 1 の実施形態のス

テップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。暗号化装置 2 0 の暗号化パラメータ生成部 2 3 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 2 4 に送出する。

[0477] 暗号文生成部 2 4 は、これらの乱数 r, s, t, k, θ 、復号装置 5 0 の公開鍵 $p k_j$ 、及び公開パラメータを用いて、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 $C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}$ を生成する (S T 2 2')。

[数116]

$$\begin{aligned} C_{2X}' &= Y_{2j}^s, C_{2X}'' = Y_{2j}^{rs}, C_{2Y}' = X_j^t, C_{2Y}'' = X_j^{rt}, \\ C_{2Z}' &= Y_{2j}^k, C_{2Z}'' = Y_{2j}^{rk}, C_{2Z1}' = X_j^k, C_{2Z1}'' = X_j^{rk}, \\ C_{2X} &= X_j^r, C_{2Y} = Y_{1j}^r, C_{2Z} = Z_j^r, C_{2Z1} = Z_{1j}^r, \\ C_3 &= e(g_4 g_5, g)^r \cdot m, C_4 = (u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v)^r, \\ C_{5X} &= (g_4 \cdot g_3^\theta)^{\frac{1}{s}}, C_{5Y} = g_3^{\frac{\theta+1}{t}}, C_{5Z} = (g_4 \cdot g_3^{\theta+1})^{\frac{1}{k}} \end{aligned}$$

[0478] ステップ S T 2 2' の終了後、暗号文生成部 2 4 は、上記全ての暗号化データ $C_{2X}' \sim C_{5Z}$ と復号装置 5 0 の識別情報 j を含む暗号文データ $C_j = (C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, j)$ を生成し、得られた暗号文データを一時データ記憶部 2 1 に書き込む。

[0479] 通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_j を復号装置 5 0 に送信する (S T 2 4')。

[0480] 復号装置 5 0 の復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と一時データ記憶部 5 2 内の公開パラメータ $p a r$ を用い、一時データ記憶部 5 2 内の再暗号文データ C_j を次の検証式 (式 (d 7)) により検証する (S T 5 1')。

[0481] なお、後述するように、ステップS T 5 1' において、復号処理部5 4は、一時データ記憶部5 2内の再暗号文データ C_j に含まれている再暗号化鍵生成装置3 0の識別情報 j により特定される復号装置5 0の公開鍵 $p k_j$ を用いても良い。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。

[数117]

$$\begin{aligned}
 e(C''_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C'_{2X}, C_4), \\
 e(C''_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C'_{2Y}, C_4), \\
 e(C''_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C'_{2Z}, C_4), \\
 e(C''_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C'_{2Z1}, C_4), \\
 e(C_{5Z}, C'_{2Z}) &= e(C_{5X}, C'_{2X}) \cdot e(g_2, g_3)^{y_j}, \\
 e(C_{5Z}, C'_{2Z1}) &= e(C_{5Y}, C'_{2Y}) \cdot e(g, g_4)^{x_j}, \\
 e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g, C_4)^{x_j}, \\
 e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g_1, C_4)^{y_j}, \\
 e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g, C_4)^{z_j}, \\
 e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g_1, C_4)^{z_j}. \dots (d 7)
 \end{aligned}$$

[0482] ここで、式(d 7)の5番目の検証式に代えて、前述した式(d 2)又は式(d 3)に示す検証式を用いても良い。また、式(d 7)の6番目の検証式に代えて、前述した式(d 4)又は式(d 5)に示す検証式を用いても良い。また、式(d 7)の7～10番目の検証式に代えて以下に示す検証式を用いても良い。

[数118]

$$\begin{aligned} e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(X_j, C_4), \\ e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Y_{1j}, C_4), \\ e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Z_j, C_4), \\ e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Z_{1j}, C_4). \end{aligned}$$

[0483] 式(d7)の10個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。

[0484] 検証が成功した場合（又はステップST51'の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 s_{k_j} と一時データ記憶部52内の公開パラメータ $p_a r$ 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119]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(1+\alpha+\theta)/k}, g^{\beta y_j r k})}{e(g^{\pi(\alpha+\theta)/s}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi(1+\alpha+\theta)/k}, g^{x_j r k})}{e(g^{\pi(\theta+1)/t}, g^{x_j r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(1+\alpha+\theta)}, g^{\beta r})}{e(g^{\pi(\alpha+\theta)}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{\pi(1+\alpha+\theta)}, g^r)}{e(g^{\pi(\theta+1)}, g^r)} \right) \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0485] (第8の実施形態)

本実施形態では、第7の実施形態において再暗号化鍵をある期間毎に更新する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施形態又は第2の実施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。

[0486] (1) 鍵セットアップ処理

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, a, r を、第7の実施形態と同様に生成する、又は外部から入手する(ST1)。ただし、 H は次式により定義されるハッシュ関数である。

[数120]

$$H : \mathbb{Z}_p^* \times \mathbb{G}^5 \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$$

[0487] 鍵生成部14は、再暗号化鍵生成装置30の識別情報を*i*としたとき、 $\mathbb{Z}_p^*$ の元 x_i, y_i, z_i, w_i を $\mathbb{Z}_p^*$ からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $sk_i = (x_i, y_i, z_i, w_i)$ とする。そして、鍵生成部14は、この秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成装置30の公開鍵 $pk_i = (X_i, Y_{1i}, Y_{2i}, Z_i, Z_{1i}, W_i)$ を生成する。ここで、

[数121]

$$\begin{aligned} X_i &= g^{x_i}, Y_{1i} = g_1^{y_i}, Y_{2i} = g_2^{y_i}, \\ Z_i &= g^{z_i}, Z_{1i} = g_1^{z_i}, W_i = g^{w_i} \end{aligned}$$

[0488] である。なお、後述する式(d10)を用いた検証処理を行わない場合には、データ Y_{2i} を省略してもよい。すなわち、公開鍵 pk_i は、データ $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ を含んでいればよい。

[0489] さらに、鍵生成部14は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = (X_{3i}, Y_{5i})$ を生成する(ST3)。ここで、

[数122]

$$X_{3i} = g_3^{x_i}, Y_{5i} = g_5^{y_i}$$

[0490] である。

[0491] また同様に、鍵生成部14は、復号装置50の識別情報を*j*としたとき、 $\mathbb{Z}_p^*$ の元 x_j, y_j, z_j, w_j を $\mathbb{Z}_p^*$ からランダムに選択し、復号装置50の秘密鍵 $sk_j = (x_j, y_j, z_j, w_j)$ とする。そして、鍵生成部14は、この秘密鍵 sk_j と公開パラメータ par を用いて復号装置50の公開鍵 $pk_j = (X_j, Y_{1j}, Y_{2j}, Z_j, Z_{1j}, W_j)$ を生成する。ここで、

[数123]

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

[0492] である。前述同様に、後述する式 (d 1 0) を用いた検証処理を行わない場合には、データ Y_{2j} を省略してもよい。すなわち、公開鍵 pk_j は、データ X_j , Y_{1j} , Z_j , Z_{1j} , W_j を含んでいればよい。

[0493] さらに、鍵生成部 1 4 は、秘密鍵 sk_j と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_j = (X_{3j}, Y_{5j})$ を生成する (S T 6)。ここで、

[数124]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

[0494] である。

[0495] (2) 暗号化処理

本実施形態においては、使い捨て署名を用いないため、第 1 の実施形態のステップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。

[0496] 暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、乱数 $r \in \mathbb{Z}_p^*$ を生成して暗号文生成部 2 4 に送出する。

[0497] 暗号文生成部 2 4 は、この乱数 r 、再暗号化鍵生成装置 3 0 の公開鍵 pk_j 、公開パラメータ par 、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_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 , C_4 を生成する (S T 2 2)。

[数125]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, C_{2F} = F_i(L)^r, \\ C_3 = e(g_4 g_5, g)^r \cdot m, C_4 = (u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v)^r$$

[0498] なお、暗号文生成部 24 は、ハッシュ関数 H への入力として時間パラメータ L を含めなくても良い。つまり、 $H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)$ の代わりに $H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)$ を計算しても良い。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。

[0499] また、ここで、関数 $F_i(L)$ は次式により定義される。

[数126]

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

[0500] ステップ S T 22 の終了後、暗号文生成部 24 は、時間パラメータ L 及び上記全ての暗号化データ $C_{2X} \sim C_4$ を含む暗号文データ $C_i = (L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4)$ 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。

[0501] 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)。

[0502] (3) 再暗号化鍵生成処理

今、復号装置 50 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 30 (図 8 の例では、グループ管理者) 宛の、時間パラメータの値として L を用いて生成された暗号文を、復号装置 50 (図 8 の例では、例えばユーザ A) 宛の暗号文に再暗号化すること (つまり、暗号文の復号権限のユーザ A へ移譲すること) を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部 32 に書き込む (S T 31)。

[0503] 乱数生成部 36 は、3 つの乱数 $\theta, \delta_x, \delta_y \in \mathbb{Z}_p^*$ を生成して再暗号化鍵生成部 34 に送出する。

[0504] 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 の再暗号化鍵生成鍵 $r k_j$ 、公開パラメータ $p a r$ 、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 (S T 3 2)。

[0505] $R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$

ここで、

[数127]

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i\delta_x}, R_{ijL5} = g_1^{y_i\delta_y} = g^{\alpha y_i\delta_y}$$

[0506] 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。

[0507] (4) 再暗号化处理

再暗号化装置 40 の再暗号化处理部 44 は、公開パラメータ $p a r$ 、一時データ記憶部 42 内の暗号文データ C_i に含まれている時間パラメータ L 、及び再暗号化鍵生成装置 30 の公開鍵 $p k_i$ を用い、一時データ記憶部 42 内の暗号文データ C_i を次の検証式により検証する (S T 4 1)。

[数128]

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

[0508] なお、ハッシュ関数Hへの入力として時間パラメータLが含まれていない場合、 $H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)$ の代わりに $H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)$ を計算して上記検証を行う。これは、後述の暗号文データや再暗号文データの検証処理においても同様である。

[0509] 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。

[0510] 検証が成功した場合（又はステップS T 4 1の検証処理をスキップした場合）、再暗号化パラメータ生成部4 5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4 4に送出する。

[0511] 再暗号化処理部4 4は、これらの乱数 s, t, k, h 、一時データ記憶部4 2に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ijL} 、再暗号化鍵生成装置3 0の公開鍵 pk_i 、及び公開パラメータ par 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（S T 4 2）。

[数129]

$$\begin{aligned}
C'_{2X} &= X_i^s, C''_{2X} = C_{2X}^s = X_i^{rs}, C'_{2Y} = Y_{1i}^t, C''_{2Y} = C_{2Y}^t = Y_{1i}^{rt}, \\
C'_{2Z} &= Z_i^k, C''_{2Z} = C_{2Z}^k = Z_i^{rk}, C'_{2Z1} = Z_{1i}^k, C''_{2Z1} = C_{2Z1}^k = Z_{1i}^{rk}, \\
C'_{2F} &= F_i(L)^h, C''_{2F} = C_{2F}^h = F_i(L)^{rh}, \\
C_{5X} &= R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}}, \\
C_{5FX} &= R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}
\end{aligned}$$

[0512] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_{2X}' \sim C_{5FY}$ と再暗号化鍵生成装置3 0の識別情報 i を、暗号文データ C_i に付加して再暗号文データ $C_j = (L, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, i)$ を生成し、得られた暗号文データを一時データ記憶部4 2に書き込む。

[0513] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する(S T 4 3)。

[0514] (5) 復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ 、一時データ記憶部5 2内の公開パラメータ $p a r$ 、及び一時データ記憶部5 2内の再暗号文データ C_j に含まれている再暗号化鍵生成装置3 0の識別情報 i により特定される再暗号化鍵生成装置3 0の公開鍵 $p k_i$ を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する(S T 5 1)。

[数130]

$$\begin{aligned}
& e(C_{2X}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2X}', C_4), \\
& e(C_{2Y}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2Y}', C_4), \\
& e(C_{2Z}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2Z}', C_4), \\
& e(C_{2Z1}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2Z1}', C_4), \\
& e(C_{2F}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2F}', C_4), \\
& e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') = e(C_{5X}, C_{2X}') \cdot e(g_2, g_3)^{y_j}, \\
& e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(g, g_4)^{x_j}, \\
& e(C_{2X}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(X_i, C_4), \\
& e(C_{2Y}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(Y_{1i}, C_4), \\
& e(C_{2Z}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(Z_i, C_4), \\
& e(C_{2Z1}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(Z_{1i}, C_4), \\
& e(C_{2F}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(F_i(L), C_4). \dots (d8)
\end{aligned}$$

ここで、式 (d8) の6番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') = e(C_{5X}, C_{2X}') \cdot e(g_5, g)^{y_j}. \dots (d9)$$

また、式 (d8) の6番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') = e(C_{5X}, C_{2X}') \cdot e(Y_{2j}, g_3). \dots (d10)$$

この場合、復号処理部54は、自装置50の公開鍵 $p k_j$ を用いて検証を行う。

式 (d8) の7番目の検証式に代えて、検証式(d11)又は(d12)を用いても良い。

$$e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(g_3, g_1)^{x_j}. \dots (d11)$$

$$e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4). \dots (d12)$$

この場合、復号処理部54は、自装置50の公開鍵 $p k_j$ を用いて検証を行う。

[0515] 式 (d8) の12個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。

[0516] 検証が成功した場合（又はステップS T 5 1の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 $s k_j$ と一時データ記憶部52内の公開パラメータ $p a r$ 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 5 2）。

[数131]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e\left(g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i k}}, g^{z_i r k}\right) \cdot e\left(g^{\frac{x_i \delta_x}{h}}, g^{(L + w_i) r h}\right)}{e\left(g^{\frac{(\pi(x_j + \theta)/x_i + (L + w_i) \delta_x)}{s}}, g^{x_i r s}\right)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e\left(g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i k}}, g^{\alpha z_i r k}\right) \cdot e\left(g^{\frac{\alpha y_i \delta_y}{h}}, g^{(L + w_i) r h}\right)}{e\left(g^{\frac{(\pi(\beta y_j + \theta)/y_i + (L + w_i) \delta_y)}{t}}, g^{\alpha y_i r t}\right)} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e\left(g^{\pi(x_j + \beta y_j + \theta)}, g^r\right) \cdot e\left(g^{x_i \delta_x}, g^{(L + w_i) r}\right)}{e\left(g^{\pi(x_j + \theta) + (L + w_i) x_i \delta_x}, g^r\right)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e\left(g^{\pi(x_j + \beta y_j + \theta)}, g^{\alpha r}\right) \cdot e\left(g^{\alpha y_i \delta_y}, g^{(L + w_i) r}\right)}{e\left(g^{\pi(\beta y_j + \theta) + (L + w_i) y_i \delta_y}, g^{\alpha r}\right)} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0517] 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 、再暗号化鍵生成鍵 $r k_j$ 、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7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、ある期間において移譲元（図8の例では、グループ管理者）向けの

暗号文についての復号権限を一度移譲先（図 8 の例では、例えばユーザ A）へ移譲した後も、次の期間については当該移譲元向けの暗号文についての復号権限を当該移譲先に与えない、つまり、（当該移譲元向けの暗号文についての）当該移譲先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。

[0518] また、上述したように本実施形態によれば、第 2 の実施形態における使い捨て署名 σ を省略する構成により、第 2 の実施形態において示した実施形態に比べ、暗号文データや再暗号文データのデータサイズを削減することができる。また、本実施形態によれば、第 2 の実施形態において示した実施形態に比べ、暗号化処理や再暗号化処理に要する計算量を削減することができる。

[0519] [変形例 18]

第 8 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 8 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。

[0520] 本変形例における暗号化処理と、第 8 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'）。

[0521] 復号装置 50 は、公開パラメータ $p_a r$ と自装置 50 の秘密鍵 $s k_i$ を用いて、暗号化装置 20 において生成された暗号文データ C_i を次の検証式により検証する（ST51'）。

[数132]

$$\begin{aligned}
e(C_{2X}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{x_i}, \\
e(C_{2Y}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g_1, C_4)^{y_i}, \\
e(C_{2Z}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{z_i}, \\
e(C_{2Z1}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g_1, C_4)^{z_i}, \\
e(C_{2F}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{L+w_i}. \dots (d13)
\end{aligned}$$

[0522] なお、復号装置50は、公開パラメータ $p_a r$ と自装置50の公開鍵 $p k_i$ を用いて、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S T 4 1と同様に検証しても良い。

[0523] 式(d13)の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。

[0524] 検証が成功した場合（又はステップS T 5 1'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p_a r$ 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（S T 5 2'）。

[数133]

$$m = C_3 / e(g_4 g_5, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned}
& m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, C_{2X})^{\frac{1}{x_i}} \\
&= m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g^{x_i r})^{\frac{1}{x_i}} \\
&= m \cdot e(g_4 g_5, g)^r / e(g_4 g_5, g)^r = m.
\end{aligned}$$

[0525] [変形例 19]

変形例 18 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 8 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。

[0526] 本変形例においても、使い捨て署名を用いないため、第 1 の実施形態のステップ ST21 及びステップ ST23 に相当する処理を行わない。暗号化装置 20 の暗号化パラメータ生成部 23 は、8 つの乱数 $r, s, t, k, h, \theta, \delta_x, \delta_y \in \mathbb{Z}_p^*$ を生成して暗号文生成部 24 に送出する。

[0527] 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 pk_j 、公開パラメータ、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 $C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}$ を生成する (ST22')。

[数134]

$$\begin{aligned}
C'_{2X} &= Y_{2j}^s, C''_{2X} = Y_{2j}^{rs}, C'_{2Y} = X_j^t, C''_{2Y} = X_j^{rt}, \\
C'_{2Z} &= Y_{2j}^k, C''_{2Z} = Y_{2j}^{rk}, C'_{2Z1} = X_j^k, C''_{2Z1} = X_j^{rk}, \\
C'_{2F} &= F_j(L)^h, C''_{2F} = F_j(L)^{rh}, \\
C_{2X} &= X_j^r, C_{2Y} = Y_{1j}^r, C_{2Z} = Z_j^r, C_{2Z1} = Z_{1j}^r, C_{2F} = F_j(L)^r, \\
C_3 &= e(g_4 g_5, g)^r \cdot m, C_4 = (u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v)^r, \\
C_{5X} &= (g_4 \cdot g_3^\theta \cdot F_j(L)^{\delta_y})^{\frac{1}{s}} = g^{\frac{\pi(\alpha+\theta)+(L+w_j)\delta_y}{s}}, \\
C_{5Y} &= (g_3^{1+\theta} \cdot F_j(L)^{\delta_x})^{\frac{1}{t}} = g^{\frac{\pi(1+\theta)+(L+w_j)\delta_x}{t}}, \\
C_{5Z} &= (g_4 \cdot g_3^{1+\theta})^{\frac{1}{k}} = g^{\frac{\pi(\alpha+1+\theta)}{k}}, \\
C_{5FX} &= (Y_{2j})^{\frac{\delta_y}{h}}, C_{5FY} = (X_j)^{\frac{\delta_x}{h}}
\end{aligned}$$

[0528] ステップS T 2 2' の終了後、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 $C_{2X}' \sim C_{5FY}$ と復号装置50の識別情報jを含む暗号文データ $C_j = (L, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, j)$ 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。

[0529] 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(S T 2 4')。

[0530] 復号装置50の復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 $s k_j$ と一時データ記憶部52内の公開パラメータ $p a r$ を用い、一時データ記憶部52内の再暗号文データ C_j を次の検証式により検証する(S T 5 1')。

[数135]

$$\begin{aligned}
e(C_{2X}''', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(C_{2X}', C_4), \\
e(C_{2Y}''', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(C_{2Y}', C_4), \\
e(C_{2Z}''', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(C_{2Z}', C_4), \\
e(C_{2Z1}''', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(C_{2Z1}', C_4), \\
e(C_{2F}''', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(C_{2F}', C_4), \\
e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') &= e(C_{5X}, C_{2X}') \cdot e(g_2, g_3)^{y_j}, \\
e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') &= e(C_{5Y}, C_{2Y}') \cdot e(g, g_4)^{x_j}, \\
e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{x_j}, \\
e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g_1, C_4)^{y_j}, \\
e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{z_j}, \\
e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g_1, C_4)^{z_j}, \\
e(C_{2F}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{L+w_j}. \quad \dots (d14)
\end{aligned}$$

[0531] ここで、式 (d 1 4) の 6 番目の検証式に代えて式 (d 9) 又は式 (d 1 0) に示す検証式を用いても良い。また、式 (d 1 4) の 7 番目の検証式に代えて式 (d 1 1) 又は式 (d 1 2) に示す検証式を用いても良い。また、式 (d 1 4) の 8 ～ 1 2 番目の検証式に代えて以下に示す検証式を用いても良い。

[数136]

$$\begin{aligned}
e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(X_j, C_4), \\
e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(Y_{1j}, C_4), \\
e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(Z_j, C_4), \\
e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(Z_{1j}, C_4), \\
e(C_{2F}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(F_j(L), C_4).
\end{aligned}$$

[0532] 式(d 1 4)の1 2個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。

[0533] 検証が成功した場合（又はステップS T 5 1'の検証処理をスキップした場合）、復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ と一時データ記憶部5 2内の公開パラメータ $p a r$ 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 5 2'）。

[数137]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\frac{\pi(\alpha+1+\theta)}{k}}, g^{\beta y_j r k}) \cdot e(g^{\frac{\beta y_j \delta_y}{h}}, g^{(L+w_j) r h})}{e(g^{\frac{\pi(\alpha+\theta)+(L+w_j)\delta_y}{s}}, g^{\beta y_j r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\pi(\alpha+1+\theta)}{k}}, g^{x_j r k}) \cdot e(g^{\frac{x_j \delta_x}{h}}, g^{(L+w_j) r h})}{e(g^{\frac{\pi(1+\theta)+(L+w_j)\delta_x}{t}}, g^{x_j r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi(\alpha+1+\theta)}, g^{\beta r}) \cdot e(g^{\beta \delta_y}, g^{(L+w_j) r})}{e(g^{\pi(\alpha+\theta)+(L+w_j)\delta_y}, g^{\beta r})} \right) \cdot \left(\frac{e(g^{\pi(\alpha+1+\theta)}, g^r) \cdot e(g^{\delta_x}, g^{(L+w_j) r})}{e(g^{\pi(1+\theta)+(L+w_j)\delta_x}, g^r)} \right) \right\} \\ &= m \cdot e(g_4 g_5, g)^r / (e(g, g)^{\pi \beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0534] (第9の実施形態)

本実施形態では、第3の実施形態において使い捨て署名を省略する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施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。

[0535] (1) 鍵セットアップ処理

始めに、鍵生成装置10の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、公開パラメータ

[数138]

$$\text{par} = \{\lambda, p, \mathbb{G}, \mathbb{G}_T, g, g_1, g_2, g_3, g_4, u, v, H\}$$

[0536] を生成する、又は外部から入手する（ST1）。ここで、 $g_3 = g^\pi$ 、 $g_4 = g_1^\pi$ である。また、Hは次式により定義されるハッシュ関数である。

[数139]

$$H : \mathbb{G}^4 \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$$

[0537] 鍵生成部14は、再暗号化鍵生成装置30の識別情報を*i*としたとき、 $\mathbb{Z}_p^*$ の元 x_i, y_i, z_i を $\mathbb{Z}_p^*$ からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $sk_i = (x_i, y_i, z_i)$ とする。そして、鍵生成部14は、この秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成装置30の公開鍵 $pk_i = (X_i, Y_{1i}, Z_i, Z_{1i})$ を生成する。ここで、

[数140]

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

[0538] である。

[0539] さらに、鍵生成部14は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = (X_{3i}, Y_{2i})$ を生成する（ST3）。ここで、

[数141]

$$X_{3i} = g_3^{x_i}, Y_{2i} = g_2^{y_i}$$

[0540] である。

[0541] また同様に、鍵生成部14は、復号装置50の識別情報を*j*としたとき、 $\mathbb{Z}_p^*$ の元 x_j, y_j, z_j を $\mathbb{Z}_p^*$ からランダムに選択し、復号装置50の秘密鍵 $sk_j = (x_j, y_j, z_j)$ とする。そして、鍵生成部14は、この秘密鍵 sk_j と公開パラメータ par を用いて復号装置50の公開鍵 $pk_j = (X_j, Y_{1j}, Z_j,$

Z_{1j}) を生成する。ここで、

[数142]

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

[0542] である。

[0543] さらに、鍵生成部 14 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = (X_{3j}, Y_{2j})$ を生成する (S T 6)。ここで、

[数143]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

[0544] である。

[0545] (2) 暗号化処理

本実施形態においては、使い捨て署名を用いないため、第 1 の実施形態のステップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。

[0546] 暗号化装置 20 の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。

[0547] 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 $p k_i$ 、及び公開パラメータ $p a r$ 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_{2Y} , C_{2Z} , C_{2Z1} , C_3 , C_4 を生成する (S T 2 2)。

[数144]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_2, g)^r \cdot m, C_4 = (u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v)^r$$

[0548] ステップ S T 2 2 の終了後、暗号文生成部 24 は、上記全ての暗号化データ $C_{2X} \sim C_4$ を含む暗号文データ $C_i = (C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4)$ 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。

[0549] 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 (ST24)。

[0550] (3) 再暗号化鍵生成処理

今、復号装置 50 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 30 (図 8 の例では、グループ管理者)宛の暗号文を、復号装置 50 (図 8 の例では、例えばユーザ A)宛の暗号文に再暗号化すること (つまり、暗号文の復号権限のユーザ A へ移譲すること) を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部 32 に書き込む (ST31)。

[0551] 乱数生成部 36 は、乱数 $\theta \in Z_p^*$ を生成して再暗号化鍵生成部 34 に送出する。

[0552] 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 $s k_i$ 、一時データ記憶部 32 内の復号装置 50 の再暗号化鍵生成鍵 $r k_j$ 、及び公開パラメータ $p a r$ を用いて、再暗号化鍵 R_{ij} を次式に示すように生成する (ST32)。

[0553] $R_{ij} = (R_{ij1}, R_{ij2}, R_{ij3})$

ここで、

[数145]

$$R_{ij1} = (X_{3j} \cdot g^\theta)^{1/x_i} = g^{\frac{\pi x_j + \theta}{x_i}},$$

$$R_{ij2} = (Y_{2j} \cdot g^\theta)^{1/y_i} = g^{\frac{\beta y_j + \theta}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{2j} \cdot g^\theta)^{1/z_i} = g^{\frac{\pi x_j + \beta y_j + \theta}{z_i}}.$$

[0554] である。なお、上式では、 $g_2 = g^\beta$ と書き替えて表記している。

[0555] (4) 再暗号化処理

再暗号化装置40の再暗号化処理部44は、公開パラメータ p, a, r と再暗号化鍵生成装置30の公開鍵 p, k_i を用い、一時データ記憶部42内の暗号文データ C_i を次の検証式により検証する (ST41)。

[数146]

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

[0556] ここで、上記4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。

[0557] 検証が成功した場合（又はステップST41の検証処理をスキップした場合）、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。

[0558] 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に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ij} 、再暗号化鍵生成装置30の公開鍵 p, k_i 、及び公開パラメータ p, a, r を用いて、次式に示すように、再暗号化データ $C'_{2X}, C''_{2X}, C'_{2Y}, C''_{2Y}, C'_{2Z}, C''_{2Z}, C'_{2Z1}, C''_{2Z1}, C_{5X}, C_{5Y}, C_{5Z}$ を生成する (ST42)。

[数147]

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

[0559] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_{2X}' \sim C_{5Z}$ と再暗号化鍵生成装置3 0の識別情報 i を、暗号文データ C_i に付加して再暗号文データ $C_j = (C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, i)$ 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4 2に書き込む。

[0560] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する(S T 4 3)。

[0561] (5) 復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ 、一時データ記憶部5 2内の公開パラメータ $p a r$ 、及び一時データ記憶部5 2内の再暗号文データ C_j に含まれている再暗号化鍵生成装置3 0の識別情報 i により特定される再暗号化鍵生成装置3 0の公開鍵 $p k_i$ を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する(S T 5 1)。

[数148]

$$\begin{aligned}
e(C_{2X}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2X}', C_4), \\
e(C_{2Y}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2Y}', C_4), \\
e(C_{2Z}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2Z}', C_4), \\
e(C_{2Z1}'', u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(C_{2Z1}', C_4), \\
e(C_{5Z}, C_{2Z}') &= e(C_{5X}, C_{2X}') \cdot e(g_2, g)^{y_j}, \\
e(C_{5Z}, C_{2Z1}') &= e(C_{5Y}, C_{2Y}') \cdot e(g, g_4)^{x_j}, \\
e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(X_i, C_4), \\
e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Y_{1i}, C_4), \\
e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Z_i, C_4), \\
e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(Z_{1i}, C_4). \dots (e1)
\end{aligned}$$

ここで、式 (e 1) の 6 番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z1}') = e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4).$$

この場合、復号処理部 5 4 は、自装置 5 0 の公開鍵 $p k_j$ を用いて検証を行う。

[0562] 式 (e 1) の 10 個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。

[0563] 検証が成功した場合（又はステップ S T 5 1 の検証処理をスキップした場合）、復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と一時データ記憶部 5 2 内の公開パラメータ $p a r$ 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 5 2)。

[数149]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{(\pi x_j + \beta y_j + \theta)/z_i k}, g^{z_i r k})}{e(g^{(\pi x_j + \theta)/x_i s}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(\pi x_j + \beta y_j + \theta)/z_i k}, g^{\alpha z_i r k})}{e(g^{(\beta y_j + \theta)/y_i t}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^r)}{e(g^{\pi x_j + \theta}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^{\alpha r})}{e(g^{\beta y_j + \theta}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0564] 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 及び再暗号化鍵生成鍵 $r k_j$ に基づいて生成する構成により、第3の実施形態の効果と同様の効果を得ることができる。

[0565] また、上述したように本実施形態によれば、第3の実施形態における使い捨て署名 σ を省略する構成により、第3の実施形態において示した実施形態に比べ、暗号文データや再暗号文データのデータサイズを削減することができる。また、本実施形態によれば、第3の実施形態において示した実施形態に比べ、暗号化処理や再暗号化処理に要する計算量を削減することができる。

。

[0566] [変形例 20]

第9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9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。

[0567] 本変形例における暗号化処理と、第9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'）。

[0568] 復号装置50は、公開パラメータ*p a r*と自装置50の秘密鍵*s k_i*を用いて、暗号化装置20において生成された暗号文データ*C_i*を次の検証式により検証する（ST51'）。

[数150]

$$\begin{aligned} e(C_{2X}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g, C_4)^{x_i}, \\ e(C_{2Y}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g_1, C_4)^{y_i}, \\ e(C_{2Z}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g, C_4)^{z_i}, \\ e(C_{2Z1}, u^{H(C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3)} \cdot v) &= e(g_1, C_4)^{z_i}. \dots (e2) \end{aligned}$$

[0569] なお、復号装置50は、公開パラメータ*p a r*と自装置50の公開鍵*p k_i*を用いて、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と同様に検証しても良い。

[0570] 式（e2）の4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。

[0571] 検証が成功した場合（又はステップS T 5 1' の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（S T 5 2'）。

[数151]

$$m = C_3 / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} & m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g)^r = m. \end{aligned}$$

[0572] （第10の実施形態）

本実施形態では、第9の実施形態において再暗号化鍵をある期間毎に更新する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施形態又は第2の実施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。

[0573] （1）鍵セットアップ処理

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 $p a r$ を、第9の実施形態と同様に生成する、又は外部から入手する（S T 1）。ただし、 H は次式により定義されるハッシュ関数である。

[数152]

$$H : \mathbb{Z}_p^* \times \mathbb{G}^5 \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$$

[0574] 鍵生成部 14 は、再暗号化鍵生成装置 30 の識別情報を i としたとき、 Z_p^* の元 x_i, y_i, z_i, w_i を Z_p^* からランダムに選択し、再暗号化鍵生成装置 30 の秘密鍵 $sk_i = (x_i, y_i, z_i, w_i)$ とする。そして、鍵生成部 14 は、この秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成装置 30 の公開鍵 $pk_i = (X_i, Y_{1i}, Z_i, Z_{1i}, W_i)$ を生成する。ここで、

[数153]

$$X_i = g^{x_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, \\ Z_{1i} = g_1^{z_i}, W_i = g^{w_i}$$

[0575] である。さらに、鍵生成部 14 は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = (X_{3i}, Y_{2i})$ を生成する (ST3)。ここで、

[数154]

$$X_{3i} = g_3^{x_i}, Y_{2i} = g_2^{y_i}$$

[0576] である。

[0577] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、 Z_p^* の元 x_j, y_j, z_j, w_j を Z_p^* からランダムに選択し、復号装置 50 の秘密鍵 $sk_j = (x_j, y_j, z_j, w_j)$ とする。そして、鍵生成部 14 は、この秘密鍵 sk_j と公開パラメータ par を用いて復号装置 50 の公開鍵 $pk_j = (X_j, Y_{1j}, Z_j, Z_{1j}, W_j)$ を生成する。ここで、

[数155]

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, \\ Z_{1j} = g_1^{z_j}, W_j = g^{w_j}$$

[0578] である。さらに、鍵生成部 14 は、秘密鍵 sk_j と公開パラメータ par を用

いて再暗号化鍵生成鍵 $rk_j = (X_{3j}, Y_{2j})$ を生成する (ST6)。ここで、
[数156]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

[0579] である。

[0580] (2) 暗号化処理

本実施形態においては、使い捨て署名を用いないため、第1の実施形態のステップST21及びステップST23に相当する処理を行わない。

[0581] 暗号化装置20の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。

[0582] 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_i 、公開パラメータ par 、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_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 , C_4 を生成する (ST22)。

[数157]

$$\begin{aligned} C_{2X} &= X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_{2F} &= F_i(L)^r, C_3 = e(g_4 g_2, g)^r \cdot m, \\ C_4 &= (u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v)^r \end{aligned}$$

ここで、関数 $F_i(L)$ は次式により定義される。

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

[0583] ステップST22の終了後、暗号文生成部24は、時間パラメータ L 及び上記全ての暗号化データ $C_{2X} \sim C_4$ を含む暗号文データ $C_i = (L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4)$ 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。

[0584] 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 (ST24)。

[0585] (3) 再暗号化鍵生成処理

今、復号装置 50 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 30 (図 8 の例では、グループ管理者) 宛の、時間パラメータの値として L を用いて生成された暗号文を、復号装置 50 (図 8 の例では、例えばユーザ A) 宛の暗号文に再暗号化すること (つまり、暗号文の復号権限のユーザ A へ移譲すること) を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、復号装置 50 の再暗号化鍵生成鍵 r_{kj} を送信する。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、復号装置 50 の再暗号化鍵生成鍵 r_{kj} を取得して一時データ記憶部 32 に書き込む (ST31)。

[0586] 乱数生成部 36 は、3つの乱数 $\theta, \delta_x, \delta_y \in \mathbb{Z}_p^*$ を生成して再暗号化鍵生成部 34 に送出する。

[0587] 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_{ki} 、一時データ記憶部 32 内の復号装置 50 の再暗号化鍵生成鍵 r_{kj} 、公開パラメータ p, a, r 、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)。

[0588] $R_{ijL} = (R_{ijL1}, R_{ijL2}, R_{ijL3}, R_{ijL4}, R_{ijL5})$

ここで、

[数158]

$$\begin{aligned}
 R_{ijL1} &= (X_{3j} \cdot g^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi x_j + \theta}{x_i} + (L+w_i)\delta_x}, \\
 R_{ijL2} &= (Y_{2j} \cdot g^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\beta y_j + \theta}{y_i} + (L+w_i)\delta_y}, \\
 R_{ijL3} &= (X_{3j} \cdot Y_{2j} \cdot g^\theta)^{1/z_i} = g^{\frac{\pi x_j + \beta y_j + \theta}{z_i}}, \\
 R_{ijL4} &= g^{x_i \delta_x}, R_{ijL5} = g^{y_i \delta_y} = g^{\alpha y_i \delta_y}
 \end{aligned}$$

[0589] 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。

[0590] (4) 再暗号化処理

再暗号化装置40の再暗号化処理部44は、公開パラメータ p 、 a 、一時データ記憶部42内の暗号文データ C_i に含まれている時間パラメータ L 、及び再暗号化鍵生成装置30の公開鍵 $p k_i$ を用い、一時データ記憶部42内の暗号文データ C_i を次の検証式により検証する（ST41）。

[数159]

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

[0591] 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。

[0592] 検証が成功した場合（又はステップST41の検証処理をスキップした場合）、再暗号化パラメータ生成部45は、4つの乱数 $s, t, k, h \in \mathbb{Z}_p^*$ を生成して再暗号化処理部44に送出する。

[0593] 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に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ijL} 、再暗号化鍵生成装置30の公開鍵 $p k_i$ 、及び公開パラメータ p, a 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160]

$$\begin{aligned}
C'_{2X} &= X_i^s, C''_{2X} = C_{2X}^s = X_i^{rs}, C'_{2Y} = Y_{1i}^t, C''_{2Y} = C_{2Y}^t = Y_{1i}^{rt}, \\
C'_{2Z} &= Z_i^k, C''_{2Z} = C_{2Z}^k = Z_i^{rk}, C'_{2Z1} = Z_{1i}^k, C''_{2Z1} = C_{2Z1}^k = Z_{1i}^{rk}, \\
C'_{2F} &= F_i(L)^h, C''_{2F} = C_{2F}^h = F_i(L)^{rh}, \\
C_{5X} &= R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}}, \\
C_{5FX} &= R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}
\end{aligned}$$

[0594] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_{2X}' \sim C_{5FY}$ と再暗号化鍵生成装置3 0の識別情報 i を、暗号文データ C_i に付加して再暗号文データ $C_j = (L, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{2F}', C_{2F}'', C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, C_{5X}, C_{5Y}, C_{5Z}, C_{5FX}, C_{5FY}, i)$ を生成し、得られた暗号文データを一時データ記憶部4 2に書き込む。

[0595] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する(S T 4 3)。

[0596] (5) 復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 s_{kj} 、一時データ記憶部5 2内の公開パラメータ p_{ar} 、及び一時データ記憶部5 2内の再暗号文データ C_j に含まれている再暗号化鍵生成装置3 0の識別情報 i により特定される再暗号化鍵生成装置3 0の公開鍵 p_{ki} を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する(S T 5 1)。

[数161]

$$\begin{aligned}
& e(C_{2X}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2X}', C_4), \\
& e(C_{2Y}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2Y}', C_4), \\
& e(C_{2Z}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2Z}', C_4), \\
& e(C_{2Z1}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2Z1}', C_4), \\
& e(C_{2F}'', u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(C_{2F}', C_4), \\
& e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') = e(C_{5X}, C_{2X}') \cdot e(g_2, g)^{y_j}, \\
& e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(g, g_4)^{x_j}, \\
& e(C_{2X}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(X_i, C_4), \\
& e(C_{2Y}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(Y_{1i}, C_4), \\
& e(C_{2Z}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(Z_i, C_4), \\
& e(C_{2Z1}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(Z_{1i}, C_4), \\
& e(C_{2F}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) = e(F_i(L), C_4). \dots (e3)
\end{aligned}$$

ここで、式(e3)の7番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') = e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4).$$

この場合、復号処理部54は、自装置50の公開鍵 pk_j を用いて検証を行う。

[0597] 式(e3)の12個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。

[0598] 検証が成功した場合（又はステップST51の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 sk_j と一時データ記憶部52内の公開パラメータ par 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162]

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

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。

$$\begin{aligned} & C_3 / \left\{ \left(\frac{e(C_{5Z}, C_{2Z}'') \cdot e(C_{5FX}, C_{2F}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'') \cdot e(C_{5FY}, C_{2F}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\frac{\pi x_j + \beta y_j + \theta}{z_i k}}, g^{z_i r k}) \cdot e(g^{\frac{x_i \delta_x}{h}}, g^{(L+w_i) r h})}{e(g^{\frac{((\pi x_j + \theta)/x_i) + (L+w_i) \delta_x}{s}}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\pi x_j + \beta y_j + \theta}{z_i k}}, g^{\alpha z_i r k}) \cdot e(g^{\frac{\alpha y_i \delta_y}{h}}, g^{(L+w_i) r h})}{e(g^{\frac{((\beta y_j + \theta)/y_i) + (L+w_i) \delta_y}{t}}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\} \\ &= C_3 / \left\{ \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^r) \cdot e(g^{x_i \delta_x}, g^{(L+w_i) r})}{e(g^{\pi x_j + \theta + (L+w_i) x_i \delta_x}, g^r)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\pi x_j + \beta y_j + \theta}, g^{\alpha r}) \cdot e(g^{\alpha y_i \delta_y}, g^{(L+w_i) r})}{e(g^{\beta y_j + \theta + (L+w_i) y_i \delta_y}, g^{\alpha r})} \right)^{\frac{1}{x_j}} \right\} \\ &= m \cdot e(g_4 g_2, g)^r / (e(g, g)^{\beta r} \cdot e(g, g)^{\pi \alpha r}) = m. \end{aligned}$$

[0599] 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 、再暗号化鍵生成鍵 $r k_j$ 、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9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、ある期間において移譲元（図8の例では、グループ管理者）向けの暗号文についての復号権限を一度移譲先（図8の例では、例えばユーザA）へ移譲した後でも、次の期間については当該移譲元向けの暗号文についての復号権限を当該移譲先に与えない、つまり、（当該移譲元向けの暗号文についての）当該移譲先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。

[0600] また、上述したように本実施形態によれば、第4の実施形態における使い捨て署名 σ を省略する構成により、第4の実施形態において示した実施形態に比べ、暗号文データや再暗号文データのデータサイズを削減することがで

きる。また、本実施形態によれば、第4の実施形態において示した実施形態に比べ、暗号化処理や再暗号化処理に要する計算量を削減することができる。

[0601] [変形例21]

第10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10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。

[0602] 本変形例における暗号化処理と、第10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'）。

[0603] 復号装置50は、公開パラメータ*p a r*と自装置50の秘密鍵*s k_i*を用いて、暗号化装置20において生成された暗号文データ*C_i*を次の検証式により検証する（ST51'）。

[数163]

$$\begin{aligned} e(C_{2X}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{x_i}, \\ e(C_{2Y}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g_1, C_4)^{y_i}, \\ e(C_{2Z}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{z_i}, \\ e(C_{2Z1}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g_1, C_4)^{z_i}, \\ e(C_{2F}, u^{H(L, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3)} \cdot v) &= e(g, C_4)^{L+w_i}. \end{aligned}$$

[0604] なお、復号装置 50 は、公開パラメータ $p_a r$ と自装置 50 の公開鍵 $p k_i$ を用いて、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 S T 4 1 と同様に検証しても良い。

[0605] 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。

[0606] 検証が成功した場合（又はステップ S T 5 1' の検証処理をスキップした場合）、復号装置 50 は、自装置 50 の秘密鍵 $s k_i$ と公開パラメータ $p_a r$ 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（S T 5 2'）。

[数164]

$$m = C_3 / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, C_{2X})^{\frac{1}{x_i}} \\ = m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g^{x_i r})^{\frac{1}{x_i}} \\ = m \cdot e(g_4 g_2, g)^r / e(g_4 g_2, g)^r = m. \end{aligned}$$

[0607] （第 1 1 の実施形態）

本実施形態では、第 5 の実施形態において使い捨て署名を省略する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第 1 の実施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。

[0608] （1）鍵セットアップ処理

始めに、鍵生成装置 10 の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、公開パラメ

ータ

[数165]

$$\text{par} = \{\lambda, p, \mathbb{G}, \mathbb{G}_T, g, g_1, u, v, H\}$$

[0609] を生成する、又は外部から入手する（ST1）。ここで、Hは次式により定義されるハッシュ関数である。

[数166]

$$H : \mathbb{G} \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$$

[0610] 鍵生成部14は、再暗号化鍵生成装置30の識別情報を*i*としたとき、 $\mathbb{Z}_p^*$ の元 x_i を $\mathbb{Z}_p^*$ からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $sk_i = x_i$ とする。そして、鍵生成部14は、この秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成装置30の公開鍵 $pk_i = X_i$ を生成する。ここで、

[数167]

$$X_i = g^{x_i}$$

[0611] である。

[0612] さらに、鍵生成部14は、秘密鍵 sk_i と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_i = X_{1i}$ を生成する（ST3）。ここで、

[数168]

$$X_{1i} = g_1^{x_i}$$

[0613] である。

[0614] また同様に、鍵生成部14は、復号装置50の識別情報を*j*としたとき、 $\mathbb{Z}_p^*$ の元 x_j を $\mathbb{Z}_p^*$ からランダムに選択し、復号装置50の秘密鍵 $sk_j = x_j$ とする。そして、鍵生成部14は、この秘密鍵 sk_j と公開パラメータ par を用

いて復号装置 50 の公開鍵 $pk_j = X_j$ を生成する。ここで、

[数169]

$$X_j = g^{x_j}$$

[0615] である。

[0616] さらに、鍵生成部 14 は、秘密鍵 sk_j と公開パラメータ par を用いて再暗号化鍵生成鍵 $rk_j = X_{1j}$ を生成する (ST6)。ここで、

[数170]

$$X_{1j} = g_1^{x_j}$$

[0617] である。

[0618] (2) 暗号化处理

本実施形態においては、使い捨て署名を用いないため、第1の実施形態のステップST21及びステップST23に相当する処理を行わない。

[0619] 暗号化装置 20 の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。

[0620] 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_j 、及び公開パラメータ par 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_2, C_3, C_4 を生成する (ST22)。

[数171]

$$C_2 = X_i^r, C_3 = e(g_1, g)^r \cdot m, C_4 = (u^{H(C_2, C_3)} \cdot v)^r$$

[0621] ステップST22の終了後、暗号文生成部 24 は、上記全ての暗号化データ $C_2 \sim C_4$ を含む暗号文データ $C_i = (C_2, C_3, C_4)$ 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。

[0622] 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 (ST24)。

[0623] (3) 再暗号化鍵生成処理

今、復号装置 50 (図 8 の例では、例えばユーザ A) が、再暗号化鍵生成装置 30 (図 8 の例では、グループ管理者)宛の暗号文を、復号装置 50 (図 8 の例では、例えばユーザ A)宛の暗号文に再暗号化すること(つまり、暗号文の復号権限のユーザ A へ移譲すること)を承諾したとする。復号装置 50 は、再暗号化鍵生成装置 30 に、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置 50 の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部 32 に書き込む (S T 31)。

[0624] 本実施形態の再暗号化鍵の生成においては、乱数を生成する必要がないため、再暗号化鍵生成装置 30 の乱数生成部 36 は不要となる。

[0625] 再暗号化鍵生成部 34 は、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 の再暗号化鍵生成鍵 $r k_j$ 、及び公開パラメータ $p a r$ を用いて、再暗号化鍵 R_{ij} を次式に示すように生成する (S T 32)。

[数172]

$$R_{ij} = X_{1j}^{1/x_i} = g_1^{\frac{x_j}{x_i}}$$

[0626] (4) 再暗号化処理

再暗号化装置 40 の再暗号化処理部 44 は、公開パラメータ $p a r$ と再暗号化鍵生成装置 30 の公開鍵 $p k_i$ を用い、一時データ記憶部 42 内の暗号文データ C_i を次の検証式により検証する (S T 41)。

[数173]

$$e(C_2, u^{H(C_2, C_3)} \cdot v) = e(X_i, C_4).$$

[0627] ここで、上記の検証式が成立すれば検証は成功し、上記の検証式が成立し

なければ検証は失敗する。

[0628] 検証が成功した場合（又はステップS T 4 1の検証処理をスキップした場合）、再暗号化パラメータ生成部4 5は、乱数 $t \in \mathbb{Z}_p^*$ を生成して再暗号化処理部4 4に送出する。

[0629] 再暗号化処理部4 4は、この乱数 t 、一時データ記憶部4 2に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ij} 、再暗号化鍵生成装置3 0の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ を用いて、次式に示すように、再暗号化データ C_2' 、 C_2'' 、 C_2''' を生成する（S T 4 2）。

[数174]

$$C_2' = X_i^t, C_2'' = R_{ij}^{1/t} = g_1^{\frac{x_j}{tx_i}}, C_2''' = C_2^t = X_i^{rt}$$

[0630] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_2' \sim C_2'''$ と再暗号化鍵生成装置3 0の識別情報 i を、暗号文データ C_i に付加して再暗号文データ $C_j = (C_2', C_2'', C_2''', C_2, C_3, C_4, i)$ 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4 2に書き込む。

[0631] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する（S T 4 3）。

[0632] （5）復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ 、一時データ記憶部5 2内の公開パラメータ $p a r$ 、及び一時データ記憶部5 2内の再暗号文データ C_j に含まれている再暗号化鍵生成装置3 0の識別情報 i により特定される再暗号化鍵生成装置3 0の公開鍵 $p k_i$ を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する（S T 5 1）。

[数175]

$$\begin{aligned}
 e(C'_2, C''_2) &= e(g, g_1)^{x_j}, \\
 e(C'''_2, u^{H(C_2, C_3)} \cdot v) &= e(C'_2, C_4), \\
 e(C_2, u^{H(C_2, C_3)} \cdot v) &= e(X_i, C_4). \quad \dots (f1)
 \end{aligned}$$

ここで、式 (f1) の1番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C'_2, C''_2) = e(X_j, g_1) \quad \dots (f2)$$

この場合、復号処理部54は、自装置50の公開鍵 $p k_j$ を用いて検証を行う。

[0633] 式 (f1) の3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。

[0634] 検証が成功した場合（又はステップST51の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 $s k_j$ と一時データ記憶部52内の公開パラメータ $p a r$ 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176]

$$m = C_3 / e(C''_2, C'''_2)^{1/x_j}$$

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。

$$\begin{aligned}
 &C_3 / e(C''_2, C'''_2)^{1/x_j} \\
 &= C_3 / e(g_1^{\frac{x_j}{tx_i}}, g^{x_i r t})^{1/x_j} \\
 &= m \cdot e(g_1, g)^r / e(g_1^{x_j}, g^r)^{1/x_j} = m.
 \end{aligned}$$

[0635] 上述したように本実施形態によれば、再暗号化鍵 R_{ij} を再暗号化鍵生成鍵 r

k_j に基づいて生成する構成により、第5の実施形態の効果と同様の効果を得ることができる。

[0636] また、上述したように本実施形態によれば、第5の実施形態における使い捨て署名 σ を省略する構成により、第5の実施形態において示した実施形態に比べ、暗号文データや再暗号文データのデータサイズを削減することができる。また、本実施形態によれば、第5の実施形態において示した実施形態に比べ、暗号化処理や再暗号化処理に要する計算量を削減することができる。

[0637] [変形例22]

第11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11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。

[0638] 本変形例における暗号化処理と、第11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')。

[0639] 復号装置50は、公開パラメータ p, r と自装置50の秘密鍵 s, k_i を用いて、暗号化装置20において生成された暗号文データ C_i を次の検証式により検証する(ST51')。

[数177]

$$e\left(C_2, u^{H(C_2, C_3)} \cdot v\right) = e(g, C_4)^{x_i} \quad \dots (f3)$$

[0640] なお、復号装置 50 は、公開パラメータ $p a r$ と自装置 50 の公開鍵 $p k_i$ を用いて、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 S T 4 1 と同様に検証しても良い。

[0641] 式 (f 3) の検証式が成立すれば検証は成功し、式 (f 3) の検証式が成立しなければ検証は失敗する。

[0642] 検証が成功した場合（又はステップ S T 5 1' の検証処理をスキップした場合）、復号装置 50 は、自装置 50 の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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（S T 5 2' ）。

[数178]

$$m = C_3 / e(C_2, g_1)^{1/x_i}$$

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。

$$\begin{aligned} C_3 / e(g_1, C_2)^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^r / e(g_1, g^{x_i r})^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^r / e(g_1, g)^r = m. \end{aligned}$$

[0643] [変形例 2 3]

変形例 2 2 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 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。

[0644] 本変形例においても、使い捨て署名を用いないため、第 1 の実施形態のス

テップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、2 つの乱数 $r, t \in \mathbb{Z}_p^*$ を生成して暗号文生成部 2 4 に送出する。

[0645] 暗号文生成部 2 4 は、これらの乱数 r, t 、復号装置 5 0 の公開鍵 $p k_j$ 、及び公開パラメータを用いて、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_2', C_2'', C_2''' , C_2, C_3, C_4 を生成する (S T 2 2')。

[数179]

$$C_2' = X_j^t, C_2'' = g_1^{1/t}, C_2''' = X_j^{rt}, C_2 = X_j^r, \\ C_3 = e(g_1, g)^r \cdot m, C_4 = (u^{H(C_2, C_3)} \cdot v)^r$$

[0646] ステップ S T 2 2' の終了後、暗号文生成部 2 4 は、上記全ての暗号化データ $C_2' \sim C_4$ と復号装置 5 0 の識別情報 j を含む暗号文データ $C_j = (C_2', C_2'', C_2''', C_2, C_3, C_4, j)$ を生成し、得られた暗号文データを一時データ記憶部 2 1 に書き込む。

[0647] 通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_j を復号装置 5 0 に送信する (S T 2 4')。

[0648] 復号装置 5 0 の復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と一時データ記憶部 5 2 内の公開パラメータ $p a r$ を用い、一時データ記憶部 5 2 内の再暗号文データ C_j を次の検証式により検証する (S T 5 1')。

[数180]

$$\begin{aligned}
 e(C_2', C_2'') &= e(g, g_1)^{x_j}, \\
 e(C_2''', u^{H(C_2, C_3)} \cdot v) &= e(C_2', C_4), \\
 e(C_2, u^{H(C_2, C_3)} \cdot v) &= e(g, C_4)^{x_j}. \quad \dots (f4)
 \end{aligned}$$

ここで、式 (f4) の1番目の検証式に代えて式 (f2) に示した検証式を用いても良い。また、式 (f4) の3番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_2, u^{H(C_2, C_3)} \cdot v) = e(X_j, C_4).$$

[0649] 式 (f4) の3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。

[0650] 検証が成功した場合（又はステップST51'の検証処理をスキップした場合）、復号装置50は、自装置50の秘密鍵 s_{k_j} と公開パラメータ p, r 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（ST52'）。

[数181]

$$m = C_3 / e(C_2'', C_2''')^{1/x_j}$$

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。

$$\begin{aligned}
 &C_3 / e(C_2'', C_2''')^{1/x_j} \\
 &= C_3 / e(g_1^{1/t}, g^{x_j r t})^{1/x_j} \\
 &= m \cdot e(g_1, g)^r / e(g_1, g^r) = m.
 \end{aligned}$$

[0651] （第12の実施形態）

本実施形態では、第11の実施形態において再暗号化鍵をある期間毎に更新する例を説明する。以下、本実施形態における鍵セットアップ処理、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、前述の第1の実施形態又は第2の実施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。

[0652] (1) 鍵セットアップ処理

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 $p a r$ を、第11の実施形態と同様に生成する、又は外部から入手する (S T 1)。ただし、 H は次式により定義されるハッシュ関数である。

[数182]

$$H : \mathbb{Z}_p^* \times \mathbb{G}^2 \times \mathbb{G}_T \rightarrow \mathbb{Z}_p^*$$

[0653] 鍵生成部14は、再暗号化鍵生成装置30の識別情報を i としたとき、 $\mathbb{Z}_p^*$ の元 x_i, y_i を $\mathbb{Z}_p^*$ からランダムに選択し、再暗号化鍵生成装置30の秘密鍵 $s k_i = (x_i, y_i)$ とする。そして、鍵生成部14は、この秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成装置30の公開鍵 $p k_i = (X_i, Y_i)$ を生成する。ここで、

[数183]

$$X_i = g^{x_i}, Y_i = g^{y_i}$$

[0654] である。

[0655] さらに、鍵生成部14は、秘密鍵 $s k_i$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_i = X_{1i}$ を生成する (S T 3)。ここで、

[数184]

$$X_{1i} = g_1^{x_i}$$

[0656] である。

[0657] また同様に、鍵生成部14は、復号装置50の識別情報を j としたとき、 $\mathbb{Z}_p^*$ の元 x_j, y_j を $\mathbb{Z}_p^*$ からランダムに選択し、復号装置50の秘密鍵 $s k_j = ($

x_j, y_j) とする。そして、鍵生成部 14 は、この秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて復号装置 50 の公開鍵 $p k_j = (X_j, Y_j)$ を生成する。ここで、

[数185]

$$X_j = g^{x_j}, Y_j = g^{y_j}$$

[0658] である。

[0659] さらに、鍵生成部 14 は、秘密鍵 $s k_j$ と公開パラメータ $p a r$ を用いて再暗号化鍵生成鍵 $r k_j = X_{ij}$ を生成する (S T 6)。ここで、

[数186]

$$X_{1j} = g_1^{x_j}$$

[0660] である。

[0661] (2) 暗号化処理

本実施形態においては、使い捨て署名を用いないため、第 1 の実施形態のステップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。

[0662] 暗号化装置 20 の暗号化パラメータ生成部 23 は、乱数 $s \in Z_p^*$ を生成して暗号文生成部 24 に送出する。

[0663] 暗号文生成部 24 は、この乱数 s 、再暗号化鍵生成装置 30 の公開鍵 $p k_i$ 、公開パラメータ $p a r$ 、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_1, C_2, C_3, C_4 を生成する (S T 2 2)。

[数187]

$$C_1 = X_i^s, \quad C_2 = F_i(L)^s, \quad C_3 = e(g_1, g)^s \cdot m, \\ C_4 = (u^{H(L, C_1, C_2, C_3)} \cdot v)^s$$

ここで、関数 $F_i(L)$ は次式により定義される。

$$F_i(L) = g^L \cdot Y_i = g^{L+y_i} \quad (L \in \mathbb{Z}_p^*)$$

[0664] ステップS T 2 2の終了後、暗号文生成部24は、時間パラメータL及び上記全ての暗号化データ $C_1 \sim C_4$ を含む暗号文データ $C_i = (L, C_1, C_2, C_3, C_4)$ 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。

[0665] 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 2 4)。

[0666] (3) 再暗号化鍵生成処理

今、復号装置50(図8の例では、例えばユーザA)が、再暗号化鍵生成装置30(図8の例では、グループ管理者)宛の、時間パラメータの値としてLを用いて生成された暗号文を、復号装置50(図8の例では、例えばユーザA)宛の暗号文に再暗号化すること(つまり、暗号文の復号権限のユーザAへ移譲すること)を承諾したとする。復号装置50は、再暗号化鍵生成装置30に、復号装置50の再暗号化鍵生成鍵 $r k_j$ を送信する。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、復号装置50の再暗号化鍵生成鍵 $r k_j$ を取得して一時データ記憶部32に書き込む(S T 3 1)。

[0667] 乱数生成部36は、乱数 $r \in \mathbb{Z}_p^*$ を生成して再暗号化鍵生成部34に送出する。

[0668] 再暗号化鍵生成部34は、この乱数 r 、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の再暗号化鍵生成鍵 $r k_j$ 、公開パラメータ $p a r$ 、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（S T 3 2）。

[0669] $R_{ijL} = (A_{ijL}, B_{ijL})$

ここで、

[数188]

$$A_{ijL} = (X_{1j}^{1/x_i} \cdot (g^{L+y_i})^r, B_{ijL} = g^{x_i r}$$

[0670] である。

[0671] （４）再暗号化处理

再暗号化装置 4 0 の再暗号化处理部 4 4 は、公開パラメータ $p a r$ 、一時データ記憶部 4 2 内の暗号文データ C_i に含まれている時間パラメータ L 、及び再暗号化鍵生成装置 3 0 の公開鍵 $p k_i$ を用い、一時データ記憶部 4 2 内の暗号文データ C_i を次の検証式により検証する（S T 4 1）。

[数189]

$$e(X_i, C_4) = e(C_1, u^{H(L, C_1, C_2, C_3)} \cdot v)$$

$$e(X_i, C_2) = e(C_1, F_i(L)).$$

[0672] ここで、上記 2 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。

[0673] 検証が成功した場合（又はステップ S T 4 1 の検証処理をスキップした場合）、再暗号化パラメータ生成部 4 5 は、2 つの乱数 $t_1, t_2 \in Z_p^*$ を生成して再暗号化处理部 4 4 に送出する。

[0674] 再暗号化处理部 4 4 は、これらの乱数 t_1, t_2 、一時データ記憶部 4 2 に記憶されている、暗号文データ C_i 、再暗号化鍵 R_{ijL} 、再暗号化鍵生成装置 3 0 の公開鍵 $p k_i$ 、及び公開パラメータ $p a r$ を用いて、次式に示すように、再暗号化データ C_1', C_1'', C_1''' , C_2', C_2'', C_2''' を生成する（S T 4 2）。

[数190]

$$C_1' = X_i^{t_1}, C_1'' = (A_{ijL})^{1/t_1}, C_1''' = C_1^{t_1} = X_i^{st_1},$$

$$C_2' = F_i(L)^{t_2}, C_2'' = B_{ijL}^{1/t_2}, C_2''' = C_2^{t_2} = F_i(L)^{st_2}$$

[0675] ステップS T 4 2の終了後、再暗号化処理部4 4は、上記全ての再暗号化データ $C_1' \sim C_2'''$ と再暗号化鍵生成装置3 0の識別情報 i を、暗号文データ C_i に付加して再暗号文データ $C_j = (L, C_1', C_1'', C_1''', C_2', C_2'', C_2''', C_1, C_2, C_3, C_4, i)$ を生成し、得られた暗号文データを一時データ記憶部4 2に書き込む。

[0676] 通信部4 3は、制御部4 6に制御されて一時データ記憶部4 2内の再暗号文データ C_j を復号装置5 0に送信する(S T 4 3)。

[0677] (5) 復号処理

復号装置5 0の復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ 、一時データ記憶部5 2内の公開パラメータ $p a r$ 、及び一時データ記憶部5 2内の再暗号文データ C_j に含まれている再暗号化鍵生成装置3 0の識別情報 i により特定される再暗号化鍵生成装置3 0の公開鍵 $p k_i$ を用い、一時データ記憶部5 2内の再暗号文データ C_j を次の検証式により検証する(S T 5 1)。

[数191]

$$\begin{aligned}
e(C_1''', u^{H(L, C_1, C_2, C_3)} \cdot v) &= e(C_1', C_4), \\
e(C_2''', u^{H(L, C_1, C_2, C_3)} \cdot v) &= e(C_2', C_4), \\
e(C_1', C_1'') &= e(g, g_1)^{x_j} \cdot e(C_2', C_2''), \\
e(X_i, C_4) &= e(C_1, u^{H(L, C_1, C_2, C_3)} \cdot v) \\
e(X_i, C_2) &= e(C_1, F_i(L)). \quad \dots (f5)
\end{aligned}$$

ここで、式 (f 5) の3番目の検証式に代えて以下に示す検証式を用いても良い。

$$e(C_1', C_1'') = e(X_j, g_1) \cdot e(C_2', C_2'') \quad \dots (f6)$$

この場合、復号処理部54は、自装置50の公開鍵 $p k_j$ を用いて検証を行う。

[0678] 式 (f 5) の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。

[0679] 検証が成功した場合（又はステップST51の検証処理をスキップした場合）、復号処理部54は、秘密鍵記憶部51内の自装置50の秘密鍵 $s k_j$ と一時データ記憶部52内の公開パラメータ $p a r$ 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192]

$$m = C_3 \cdot (e(C_2'', C_2''')/e(C_1'', C_1'''))^{1/x_j}.$$

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。

$$\begin{aligned} & C_3 \cdot \{e(g^{x_i r/t_2}, F_i(L)^{st_2})/e((g_1^{x_j/x_i} \cdot F_i(L)^r)^{1/t_1}, g^{sx_i t_1})\}^{1/x_j} \\ &= C_3 \cdot \{e(g^{x_i r}, F_i(L)^s)/e(g_1^{x_j/x_i} \cdot F_i(L)^r, g^{sx_i})\}^{1/x_j} \\ &= C_3 \cdot \{e(g^{x_i r}, F_i(L)^s)/e(g_1^{x_j} \cdot F_i(L)^{x_i r}, g^s)\}^{1/x_j} \\ &= m \cdot e(g_1, g)^s \cdot \{1/e(g_1^{x_j}, g^s)\}^{1/x_j} = m. \end{aligned}$$

[0680] 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 r 、再暗号化鍵生成鍵 $r k_j$ 、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、ある期間において移譲元（図8の例では、グループ管理者）向けの暗号文についての復号権限を一度移譲先（図8の例では、例えばユーザA）へ移譲した後でも、次の期間については当該移譲元向けの暗号文についての復号権限を当該移譲先に与えない、つまり、（当該移譲元向けの暗号文についての）当該移譲先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。

[0681] また、上述したように本実施形態によれば、第6の実施形態における使い捨て署名 σ を省略する構成により、第6の実施形態において示した実施形態に比べ、暗号文データや再暗号文データのデータサイズを削減することができる。また、本実施形態によれば、第6の実施形態において示した実施形態に比べ、暗号化処理や再暗号化処理に要する計算量を削減することができる。

[0682] [変形例24]

第12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 12 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。

[0683] 本変形例における暗号化処理と、第 12 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')。

[0684] 復号装置 50 は、公開パラメータ $p a r$ と自装置 50 の秘密鍵 $s k_i$ を用いて、暗号化装置 20 において生成された暗号文データ C_i を次の検証式により検証する (ST51')。

[数193]

$$e(g, C_4)^{x_i} = e(C_1, u^{H(L, C_1, C_2, C_3)} \cdot v)$$

$$e(g, C_2)^{x_i} = e(C_1, g)^{L+y_i} \quad \dots (f7)$$

[0685] なお、復号装置 50 は、公開パラメータ $p a r$ と自装置 50 の公開鍵 $p k_i$ を用いて、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 と同様に検証しても良い。

[0686] 式 (f7) の 2 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。

[0687] 検証が成功した場合 (又はステップ ST51' の検証処理をスキップした場合)、復号装置 50 は、自装置 50 の秘密鍵 $s k_i$ と公開パラメータ $p a r$ 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 (S

T 5 2') 。

[数194]

$$m = C_3 / e(C_1, g_1)^{\frac{1}{x_i}}$$

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。

$$\begin{aligned} & C_3 / e(C_1, g_1)^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^s / e(g^{x_i s}, g_1)^{\frac{1}{x_i}} \\ &= m \cdot e(g_1, g)^s / e(g, g_1)^s = m. \end{aligned}$$

[0688] [変形例 2 5]

変形例 2 4 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 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 5 0 の識別情報を j とする。

[0689] 本変形例においても、使い捨て署名を用いないため、第 1 の実施形態のステップ S T 2 1 及びステップ S T 2 3 に相当する処理を行わない。暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、2 つの乱数 $t_1, t_2 \in Z_p^*$ を生成して暗号文生成部 2 4 に送出する。

[0690] 暗号文生成部 2 4 は、これらの乱数 t_1, t_2 、復号装置 5 0 の公開鍵 $p k_j$ 、公開パラメータ、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 $C_1', C_1'', C_1''', C_2', C_2'', C_2'''$ 、 C_1, C_2, C_3, C_4 を生成する (S T 2 2') 。

[数195]

$$\begin{aligned}
C_1' &= X_j^{t_1}, C_1'' = (F_j(L) \cdot g_1)^{1/t_1}, C_1''' = X_j^{st_1}, \\
C_2' &= F_j(L)^{t_2}, C_2'' = X_j^{1/t_2}, C_2''' = F_j(L)^{st_2}, \\
C_1 &= X_j^s, C_2 = F_j(L)^s, C_3 = e(g_1, g)^s \cdot m, \\
C_4 &= (u^{H(L, C_1, C_2, C_3)} \cdot v)^s
\end{aligned}$$

[0691] ステップS T 2 2' の終了後、暗号文生成部 2 4 は、時間パラメータ L、上記全ての暗号化データ $C_1' \sim C_4$ と復号装置 5 0 の識別情報 j を含む暗号文データ $C_j = (L, C_1', C_1'', C_1''', C_2', C_2'', C_2''', C_1, C_2, C_3, C_4, j)$ を生成し、得られた暗号文データを一時データ記憶部 2 1 に書き込む。

[0692] 通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_j を復号装置 5 0 に送信する (S T 2 4')。

[0693] 復号装置 5 0 の復号処理部 5 4 は、秘密鍵記憶部 5 1 内の自装置 5 0 の秘密鍵 $s k_j$ と一時データ記憶部 5 2 内の公開パラメータ $p a r$ を用い、一時データ記憶部 5 2 内の再暗号文データ C_j を次の検証式により検証する (S T 5 1')。

[数196]

$$\begin{aligned}
e(C_1''', u^{H(L, C_1, C_2, C_3)} \cdot v) &= e(C_1', C_4), \\
e(C_2''', u^{H(L, C_1, C_2, C_3)} \cdot v) &= e(C_2', C_4), \\
e(C_1', C_1'') &= e(g, g_1)^{x_j} \cdot e(C_2', C_2''), \\
e(g, C_4)^{x_j} &= e(C_1, u^{H(L, C_1, C_2, C_3)} \cdot v) \\
e(g, C_2)^{x_j} &= e(C_1, g)^{L+y_j}. \quad \dots (f 8)
\end{aligned}$$

[0694] ここで、式 (f 8) の 3 番目の検証式に代えて式 (f 6) に示した検証式

を用いても良い。また、式（f 8）の4番目及び5番目の検証式に代えて以下に示す検証式を用いても良い。

[数197]

$$e(X_j, C_4) = e(C_1, u^{H(L, C_1, C_2, C_3)} \cdot v)$$

$$e(X_j, C_2) = e(C_1, F_j(L)).$$

[0695] 式（f 8）の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。

[0696] 検証が成功した場合（又はステップS T 5 1' の検証処理をスキップした場合）、復号処理部5 4は、秘密鍵記憶部5 1内の自装置5 0の秘密鍵 $s k_j$ と一時データ記憶部5 2内の公開パラメータ $p a r$ 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 5 2'）。

[数198]

$$m = C_3 \cdot (e(C_2'', C_2''')/e(C_1'', C_1'''))^{1/x_j}.$$

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。

$$\begin{aligned} & C_3 \cdot \{e(C_2'', C_2''')/e(C_1'', C_1''')\}^{1/x_j} \\ &= C_3 \cdot \{e(g^{x_j/t_2}, F_j(L)^{st_2})/e((F_j(L) \cdot g_1)^{1/t_1}, g^{sx_j t_1})\}^{1/x_j} \\ &= C_3 \cdot \{e(g^{x_j}, F_j(L)^s)/e(F_j(L) \cdot g_1, g^{sx_j})\}^{1/x_j} \\ &= m \cdot e(g_1, g)^s \cdot \{1/e(g_1, g^{sx_j})\}^{1/x_j} = m. \end{aligned}$$

[0697] 以上説明した少なくとも一つの実施形態によれば、再暗号化鍵を再暗号化鍵生成鍵に基づいて生成する構成により、安全なファイル共有を実現することができる。例えば、移譲先（図8の例では、例えばユーザA）が再暗号化鍵生成鍵を移譲元（図8の例では、グループ管理者）に通知しなければ再暗号化鍵が生成され得ないため、移譲先の承諾なく再暗号化（つまり、暗号文

の復号権限の当該移譲先への移譲)を行わないようにすることができる。

[0698] なお、上記の各実施形態の利用場面について以下に記載する。

[0699] 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。

[0700] (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。

[0701] (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。

[0702] (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。

[0703] 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。

[0704] (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に個別の暗号化鍵である)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。同様に、ユーザAは、(ユーザCに個別の暗号化鍵である)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。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。

[0705] (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。

[0706] (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、再暗号化鍵を用いて(ユーザAがアップロードした)暗号化ファイルを各ユーザだけが復号できる暗号化ファイルにそれぞれ再暗号化する。プロキシ再暗号化方式の詳細は後述する。

[0707] (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に個別の暗号化鍵である)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。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。

[0708] (2)の共通鍵方式では、ある時点から(その時点までファイル共有を許可していた)あるユーザがファイルを共有できないようにする(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ことや、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、全ての暗号化ファイルが(当該漏洩鍵を入手した者ならば誰でも)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。

[0709] 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すれば、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。以上のようなプロキシ再暗号化方式は、特に問題は無いが、しいて言えば、サーバが各ユーザの許可なしに再暗号文を作成可能な状態にある。このため、プロキシ再暗号化方式は、安全なファイル共有を実現する観点から、改善の余地があり、本実施形態にかかる発明は、安全なファイル共有を実現し得る。

[0710] 次に、再暗号化鍵生成用公開情報を用いる第13及び第14の実施形態について説明する。

[0711] (第13の実施形態)

第13及び第14の実施形態に関するプロキシ再暗号化の基本的なモデルは、前述同様に、5つの関数からなる。また同様に、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。

[0712] 例えば、本実施形態に示す再暗号化方式のように、公開鍵を暗号化用公開鍵と再暗号化鍵生成用公開情報に分けるモデルも考えられるが、従来の技術では、暗号化用公開鍵と再暗号化鍵生成用公開情報を分けずに行うモデルも存在している。

[0713] また、前述同様に、非相互作用的 (non-interactive) と呼ばれるモデルや、ユーザAの秘密鍵 $s k_A$ に代えて、ユーザB宛の再暗号化鍵 $r k_{A \rightarrow B}$ とユーザCの秘密鍵 $s k_C$ とが入力されるモデルなども考えられている。

[0714] また、前述同様に、一方向性 (unidirectional) と呼ばれるモデルや、双方向性 (bidirectional) と呼ばれるモデルなども知られている。

[0715] 次に、第13及び第14の実施形態に係るファイル共有システムの構成及び効果は、図7及び図8を用いて説明したファイル共有システムの構成及び効果と同様である。但し、第13及び第14の実施形態では、再暗号化鍵生成用公開情報を用いるため、図8に代えて、図18が説明に用いられる。

[0716] 図12は第13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12と図18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の暗号化用公開鍵、再暗号化鍵生成用公開情報、及び秘密鍵をそれぞれ生成する。

[0717] 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暗号化用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。

[0718] 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の再暗号化鍵生成用公開情報と乱数とを用いて再暗号化鍵を生成する。

[0719] 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。

[0720] 復号装置50は、再暗号化鍵生成装置30の暗号化用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の暗号化用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。

[0721] 図12と図18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。ユーザが自身の暗号化用公開鍵、再暗号化鍵生成用公開情報、及び秘密鍵をそれぞれ生成する場合、当該ユーザは鍵生成装置10を保持する。

[0722] 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暗号化用公開鍵、再暗号化鍵生成用公開情報、及び秘密鍵をそれぞれ生成する場合、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。

[0723] ここで、例えば、ユーザ管理者又はサーバSvが再暗号化鍵を生成する場合、ユーザ管理者又はサーバSvが再暗号化鍵生成装置30を保持する。サーバSvは、再暗号化装置40を保持する。図18に例示したファイル共有システムにおいては、サーバSvが公開鍵記憶部1、暗号文記憶部2、再暗号化鍵記憶部3及び再暗号化鍵生成用公開情報記憶部4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暗号化用公開鍵を取得している。しかし、これに限らず、後述するように、ユーザCは（暗号化に用いる暗号化用公開鍵を生成した）鍵生成装置10から暗号化に用いる暗号化用公開鍵を取得してもよい。また、サーバSv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。ここで、暗号文記憶部 2 は再暗号化装置 40 に含まれていてもよいし、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よい。

[0724] 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。そして、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、各ユーザ装置の暗号化用公開鍵、再暗号化鍵生成用公開情報、及び秘密鍵は、第 1 ユーザ装置の第 1 暗号化用公開鍵、第 1 再暗号化鍵生成用公開情報、及び第 1 秘密鍵、第 2 ユーザ装置の第 2 暗号化用公開鍵、第 2 再暗号化鍵生成用公開情報、及び第 2 秘密鍵、…とそれぞれ呼んでもよい。

[0725] 続いて、各装置 10～50 の構成を具体的に説明する。

[0726] 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、鍵生成部 14、通信部 15 及び制御部 16 を備えている。

[0727] 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。

[0728] 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。

[0729] 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。

[0730] 鍵生成部 14 は、ユーザ宛の暗号化用公開鍵、再暗号化鍵生成用公開情報、及び秘密鍵を生成する。

[0731] 通信部 15 は、鍵生成装置 10 と他の装置 20、30、40、50 とで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。

[0732] (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 の暗号化用公開鍵、再暗号化鍵生成用公開情報、及び秘密鍵を当該各装置 3

0, 50に送信する機能。

[0733] (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の暗号化用公開鍵を暗号化装置20に送信する機能。

[0734] 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。これは鍵生成装置10の他の装置20, 30, 40, 50の各通信部についても同様である。

[0735] 制御部16は、図13に示す動作を実行するように、鍵生成装置10の各部11～15を制御する機能をもっている。

[0736] 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。

[0737] 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の暗号化用公開鍵や、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」と記す）を記憶する記憶装置である。

[0738] 通信部22は、暗号化装置20と他の装置10, 30, 40, 50とで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。

[0739] (f22-1) 鍵生成装置10に公開された再暗号化鍵生成装置30の暗号化用公開鍵を取得して一時データ記憶部21に書き込む機能。

[0740] (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。

[0741] 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っている。

[0742] 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。

[0743] (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の暗号化用公開鍵（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。

[0744] (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。

[0745] 制御部 25 は、図 14 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。

[0746] 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。

[0747] 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。

[0748] 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 の再暗号化鍵生成用公開情報や、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。

[0749] 通信部 33 は、再暗号化鍵生成装置 30 と他の装置 10, 20, 40, 50 とで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。

[0750] 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。

[0751] (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 の再暗号化鍵生成用公開情報（第 2 ユーザ装置の第 2 再暗号化鍵生成用公開情報）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ー詳しくは乱数一が不要）。

[0752] ここで、再暗号化鍵を生成する機能(f34-1)は、再暗号化前の暗号文データには依存せずに、第 1 秘密鍵、第 2 再暗号化鍵生成用公開情報及び乱数に基づいて、再暗号化鍵を生成してもよい。再暗号化鍵生成装置 30 の暗号化用公開鍵は、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もよ

い。第2再暗号化鍵生成用公開情報は、第2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もよい。

[0753] (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。

[0754] 制御部35は、図15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。

[0755] 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。

[0756] 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、再暗号化处理部44、再暗号化パラメータ生成部45及び制御部46を備えている。

[0757] 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。

[0758] 一時データ記憶部42は、再暗号化处理部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。

[0759] 通信部43は、再暗号化装置40と他の装置10、20、30、50とで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。

[0760] (f43-1) 暗号化装置20から受けた暗号文データを再暗号化处理部44に送出する機能。

[0761] (f43-2) 制御部46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。

[0762] 再暗号化处理部44は、例えば、以下の各機能(f44-1)～(f44-2)をもっている。

[0763] (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。

[0764] (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。

- [0765] 制御部 46 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 16 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。
- [0766] 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 54、及び制御部 56 を備えている。
- [0767] 秘密鍵記憶部 51 は、鍵生成装置 10 から受けた自装置 50 の秘密鍵を記憶する記憶装置である。
- [0768] 一時データ記憶部 52 は、鍵生成装置 10 から受けた自装置 50 の暗号化用公開鍵・再暗号化鍵生成用公開情報及び再暗号化鍵生成装置 30 の暗号化用公開鍵や、復号処理部 54 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。
- [0769] 通信部 53 は、復号装置 50 と他の装置 10、20、30、40 とで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。
- [0770] (f53-1) 鍵生成装置 10 から受けた自装置 50 の秘密鍵を秘密鍵記憶部 51 に書き込む機能。
- [0771] (f53-2) 鍵生成装置 10 から受けた自装置 50 の暗号化用公開鍵・再暗号化鍵生成用公開情報及び再暗号化鍵生成装置 30 の暗号化用公開鍵を一時データ記憶部 52 に書き込む機能。
- [0772] (f53-3) 再暗号化装置 40 から受けた再暗号化データを復号処理部 54 に送出する機能。
- [0773] 復号処理部 54 は、例えば、以下の各機能(f54-1)～(f54-3)をもっている。
- [0774] (f54-1) 再暗号化装置 40 から再暗号文データを受けると、秘密鍵記憶部 51 から読み出した当該復号装置 50 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。
- [0775] (f54-2) 得られた平文データを一時データ記憶部 52 に書き込む機能。

[0776] 制御部 56 は、図 17 に示す動作を実行するように、各部 51～54 を制御する機能をもっている。

[0777] 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 13 乃至図 17 のシーケンス図を用いて説明する。

[0778] 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。

[0779] （１）鍵セットアップ処理は、鍵生成装置 10 により、図 13 及び以下の各ステップ ST1～ST12 に示すように実行される。

[0780] 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
 $(p, \lambda, G, G_T, g, g_1, g_2, g_3, g_4, u, v,$
 [数199]

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

[0781]) を生成する、又は外部から入手する (ST1)。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 $g, g_1, g_2, g_3, g_4, u, v$ 、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200]

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

[0782] を生成する。なお、 Z_p^* は Z_p かつ 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。

[0783] 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、位数 $p > 2^\lambda$ を満たす双線型写像群(bilinear map groups) (G, G_T) を選択する。ここで、 p は整数である。 p は素数であっても良いし、合成数であっても良い。公開パラメータ生成部 13 は、 G の元 (げん) g, g_1, g_2, u, v を G からランダムに選択する。公開パラメータ生成部 13 は、 ξ を Z_p^* からランダムに選択し、 $g_3 = g^\xi, g_4 = g_1^\xi$ を計算する。なお、 Z_p^* は Z_p かつ p と互いに素な整数の集合 ($= (Z/pZ)^*$) であり、 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。 g_3 は乱数 ξ とシステム固定値 g に基づく値である。 g_4 は乱数 ξ とシステム固定値 g_1 に基づく値である。

[0784] また、使い捨て署名アルゴリズム

[数201]

$\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ (以下、 $\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ を sig ともいう) において、 $\hat{G}$ は使い捨ての鍵ペア (s_{sk}, s_{vk}) 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。

[0785] 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。

[0786] 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。

[0787] 1. 任意の $(g, h) \in G \times G$ 及び $a, b \in Z$ について、 $e(g^a, h^b) = e(g, h)^{a \cdot b}$ が成り立つ。ここで、 Z とは整数の集合である。

[0788] 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。

[0789] 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。

[0790] 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 に関するベキ指数である。)。

[0791]
$$e(g_1 g_2, g) = e(g, g_1 g_2) = e(g, g^\alpha \cdot g^\beta) = e(g, g^{\alpha+\beta}) = e(g, g)^{\alpha+\beta} = e(g, g)^\alpha \cdot e(g, g)^\beta$$

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。

[0792] 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よい。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よい。この場合、後述する各処理における G の各元を、 G_1 の元又は G_2 の元と適宜書き換えればよい。これらは他の実施形態においても同様である。

[0793] 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 , λ , G , G_T , g , g_1 , g_2 , g_3 , g_4 , u , v , Sig を公開する (S T 2)。なお、ステップ S T 1 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、ステップ S T 1 及びステップ S T 2 をスキップしてもよい。

[0794] また、鍵生成部 14 は、再暗号化鍵生成装置 30 の識別情報を i 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 $sk_i = (x_i, y_i, z_i)$ を用いて再暗号化鍵生成装置 30 の暗号化用公開鍵

[数202]

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

[0795] を生成する (S T 7)。

[0796] ここで、

[数203]

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

[0797] である。なお、後述する変形例 27 を行わない場合には、データ Y_i を省略してもよい。すなわち、公開鍵 pk_i は、データ X_i, Y_{1i}, Z_i, Z_{1i} を含んでいればよい。

[0798] また、この秘密鍵 $sk_i = (x_i, y_i, z_i)$ を用いて再暗号化鍵生成装置 30 の再暗号化鍵生成用公開情報

[数204]

$$pi_i = (X_{3i}, Y_{2i})$$

[0799] を生成する (S T 7')。

[0800] ここで、

[数205]

$$X_{3i} = g_3^{x_i}, Y_{2i} = g_2^{y_i}$$

[0801] である。

[0802] 続いて、鍵生成部 14 は、生成した暗号化用公開鍵・再暗号化鍵生成用公

開情報・秘密鍵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 の暗号化用公開鍵 $p k_i$ を公開する (ST9)。

[0803] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j 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 の暗号化用公開鍵

[数206]

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

[0804] を生成する (ST10)。

[0805] ここで、

[数207]

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

[0806] である。前述同様に、後述する変形例 27 を行わない場合には、データ Y_j を省略してもよい。すなわち、公開鍵 $p k_j$ は、データ X_j, Y_{1j}, Z_j, Z_{1j} を含んでいけばよい。

[0807] また、この秘密鍵 $s k_j$ を用いて復号装置 50 の再暗号化鍵生成用公開情報

[数208]

$$pi_j = (X_{3j}, Y_{2j})$$

[0808] を生成する (ST10')。

[0809] ここで、

[数209]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

[0810] である。

[0811] 続いて、鍵生成部 14 は、生成した暗号化用公開鍵・再暗号化鍵生成用公開情報・秘密鍵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 $s k_j$ を復号装置 50 に送信する (ST 11)。鍵生成装置 10 は、一時データ記憶部 12 内の復号装置 50 の再暗号化鍵生成用公開情報 $p i_j$ を公開する (ST 12)。また、所望により、暗号化装置 20 の秘密鍵 $s k_h$ 、暗号化用公開鍵 $p k_h$ 及び再暗号化鍵生成用公開情報 $p i_h$ についても各ステップ ST 10～ST 12 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、暗号化用公開鍵 $p k_h$ 及び再暗号化鍵生成用公開情報 $p i_h$ を目的に応じて公開してもよい。

[0812] 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、各ステップ ST 2, ST 6, ST 9, ST 12 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。

[0813] (2) 暗号化処理は、暗号化装置 20 により、図 14 及び以下の各ステップ ST 21～ST 24 に示すように実行される。

[0814] 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210]

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

[0815] 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 ($C_1 = s v k$)。

[0816] 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 2 4 に送出する。

[0817] 暗号文生成部 2 4 は、この乱数 r 及び再暗号化鍵生成装置 3 0 の暗号化用公開鍵 $p k_i$ を用いて、平文データとしてのメッセージ $m \in G_T$ 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 2 2)。

[数211]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_2 g_4, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

[0818] ステップ S T 2 2 の終了後、暗号文生成部 2 4 は、暗号化データ C_3 , C_4 に対し、

[数212]

公開パラメータにおける署名生成機能 $\hat{S}$

[0819] とステップ S T 2 1 で生成した署名鍵 $s s k$ 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 2 3)。

[数213]

$$\sigma = \hat{S} (s s k, (C_3, C_4))$$

[0820] しかる後、暗号文生成部 2 4 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 2 1 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。

[0821] いずれにしても通信部 2 2 は、制御部 2 5 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(ST24)。

[0822] 以上により、暗号化処理が完了する。

[0823] 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。

[0824] (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15及び以下の各ステップST31～ST33に示すように実行される。

[0825] 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の再暗号化鍵生成用公開情報 p_{ij} を取得して一時データ記憶部32に書き込む(ST31)。また、通信部33は、前述したステップST5のとき、再暗号化鍵生成装置30の秘密鍵 s_{ki} を鍵生成装置10から受信して秘密鍵記憶部31に書き込んでいく。

[0826] 乱数生成部36は、乱数 $\gamma \in Z_p^*$ を生成して再暗号化鍵生成部34に送出する。

[0827] 再暗号化鍵生成部34は、この乱数 γ 、秘密鍵記憶部31内の再暗号化鍵生成装置30の秘密鍵 s_{ki} 、及び一時データ記憶部32内の復号装置50の再暗号化鍵生成用公開情報 p_{ij} 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)。

[数214]

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

[0828] ここで、

[数215]

$$R_{ij1} = (X_{3j} \cdot g^{\gamma})^{\frac{1}{x_i}} = g^{\frac{\xi x_j + \gamma}{x_i}},$$

$$R_{ij2} = (Y_{2j} \cdot g^{\gamma})^{\frac{1}{y_i}} = g^{\frac{\beta y_j + \gamma}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{2j} \cdot g^{\gamma})^{\frac{1}{z_i}} = g^{\frac{\xi x_j + \beta y_j + \gamma}{z_i}}.$$

[0829] である。なお、上式では、 $g_1 = g^{\alpha}$ 、 $g_2 = g^{\beta}$ 、 $g_3 = g^{\xi}$ 、 $g_4 = g^{\alpha \xi}$ と書き替えて表記している。

[0830] 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）。

[0831] 以上により、再暗号化鍵生成処理が完了する。

[0832] （4）再暗号化処理は、再暗号化装置40により、図16及び以下の各ステップST41～ST43に示すように実行される。

[0833] 再暗号化装置40の通信部43は、ステップST24で送信された暗号文データ C_i と、ステップST33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。

[0834] 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216]

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

[0835] 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。

[0836] 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。

[0837] 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_{5X} , C_{5Y} , C_{5Z} を生成する (ST42)。

[数217]

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

[0838] ステップST42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 $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ 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 $C_j = (C_1, C_{2X}', C_{2X}'', C_{2Y}', C_{2Y}'', C_{2Z}', C_{2Z}'', C_{2Z1}', C_{2Z1}'', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ は、検証を省略する場合、復号に用いない検証用データ $(C_1, C_{2X}', C_{2Y}', C_{2Z}', C_{2Z1}', C_4, \sigma)$ 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 $(C_{2X}', C_{2Y}', C_{2Z}', C_{2Z1}')$ を生成する処理も省略される。

[0839] いずれにしても通信部 43 は、制御部 46 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)。

[0840] 以上により、再暗号化処理が完了する。

[0841] (5) 復号処理は、復号装置 50 により、図 17 及び以下のステップ ST51 及び ST52 に示すように実行される。

[0842] 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。

[0843] 復号処理部 54 は、公開パラメータ及び自装置 50 の暗号化用公開鍵 $p k_j$ 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 (ST51)。

[数218]

$$e(C_{2X}'', u^{C_1} \cdot v) = e(C_{2X}', C_4)$$

$$e(C_{2Y}'', u^{C_1} \cdot v) = e(C_{2Y}', C_4)$$

$$e(C_{2Z}'', u^{C_1} \cdot v) = e(C_{2Z}', C_4)$$

$$e(C_{2Z1}'', u^{C_1} \cdot v) = e(C_{2Z1}', C_4)$$

$$e(C_{5Z}, C_{2Z}') = e(C_{5X}, C_{2X}') \cdot e(Y_j, g_2)$$

$$e(C_{5Z}, C_{2Z1}') = e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4)$$

$$\hat{V}(C_1, \sigma, (C_3, C_4)) = 1$$

[0844] 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。

[0845] 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219]

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

[0846] 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、 $g_1 = g^\alpha$, $g_2 = g^\beta$, $g_3 = g^\xi$, $g_4 = g^{\alpha\xi}$ と書き替えて表記している。

[数220]

$$\begin{aligned} & \frac{C_3}{\left\{ \left(\frac{e(C_{5Z}, C_{2Z}'')}{e(C_{5X}, C_{2X}'')} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}'')}{e(C_{5Y}, C_{2Y}'')} \right)^{\frac{1}{x_j}} \right\}} \\ &= \frac{C_3}{\left\{ \left(\frac{e(g^{\frac{\xi x_j + \beta y_j + \gamma}{z_i k}}, g^{z_i r k})}{e(g^{\frac{\xi x_j + \gamma}{x_i s}}, g^{x_i r s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\xi x_j + \beta y_j + \gamma}{z_i k}}, g^{\alpha z_i r k})}{e(g^{\frac{\beta y_j + \gamma}{y_i t}}, g^{\alpha y_i r t})} \right)^{\frac{1}{x_j}} \right\}} \\ &= \frac{m \cdot e(g_2 g_4, g)^r}{(e(g, g)^{\beta r} \cdot e(g, g)^{\alpha \xi r})} = m \end{aligned}$$

[0847] なお、復号処理部 54 は、ステップ S T 51 の検証処理を省略し、ステップ S T 52 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 S T 51 の検証処

理を省略し、ステップS T 5 2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k e yについて、 $m = k e y$ として、mをk e yに置き換えてもよい。この場合、共通鍵k e y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。

[0848] 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 γ 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。

[0849] 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 γ 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。

[0850] 補足すると、従来は、サーバの運営者、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の許可なく第三者が計算できてしまう不都合がある。

[0851] しかしながら、本実施形態によれば、再暗号化鍵 R_{ij} を乱数 γ に基づいて生成する構成により、サーバの運営者、ユーザB及びユーザE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。

[0852] また、本来の委譲先の再暗号化鍵生成用公開情報を用いて再暗号化鍵を生成する構成により、当該委譲先が再暗号化鍵生成用公開情報を提供しなければ再暗号化鍵は生成できない。そのため、本来の委譲先の許可の下であれば、再暗号化鍵を生成することができるようになる。

[0853] [変形例 2 6]

第 1 3 の実施形態では、暗号化装置 2 0 において暗号文データを生成し、再暗号化装置 4 0 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 5 0 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 3 の実施形態を変更してもよい。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よい。本変形例における鍵セットアップ処理は、第 1 3 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。

[0854] 本変形例における暗号化処理と、第 1 3 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 5 0 の識別情報を i とする。この場合、暗号化装置 2 0 の通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_i を復号装置 5 0 に送信する (S T 2 4')。

[0855] 復号装置 5 0 は、暗号化装置 2 0 において生成された暗号文データ C_i をステップ S T 4 1 と同様に検証する。検証が成功した場合、復号装置 5 0 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 221]

$$m = \frac{C_3}{e(g_2 g_4, C_{2X})^{\frac{1}{x_i}}}$$

[0856] なお、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。

[数222]

$$\begin{aligned}
& m \cdot e(g_2 g_4, g)^r \bigg/ e(g_2 g_4, C_{2X})^{\frac{1}{x_i}} \\
& = m \cdot e(g_2 g_4, g)^r \bigg/ e(g_2 g_4, g^{x_i r})^{\frac{1}{x_i}} \\
& = m \cdot e(g_2 g_4, g)^r \bigg/ e(g_2 g_4, g)^r = m
\end{aligned}$$

[0857] [変形例 2 7]

変形例 2 6 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よい。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よい。本変形例における鍵セットアップ処理、復号処理は、第 1 3 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 5 0 の識別情報を j とする。

[0858] 暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、ステップ S T 2 1 と同様に (s s k, s v k) を生成し (S T 2 1')、暗号化データ C₁ に検証鍵 s v k をセットする (C₁ = s v k)。

[0859] また、暗号化パラメータ生成部 2 3 は、5 つの乱数 r, s, t, k, γ ∈ Z_p* を生成して暗号文生成部 2 4 に送出する。

[0860] 暗号文生成部 2 4 は、これらの乱数 r, s, t, k, γ 及び復号装置 5 0 の暗号化用公開鍵 p k_j を用いて、平文データとしてのメッセージ m ∈ 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_{5X}, C_{5Y}, C_{5Z}, C₃, C₄ を生成する (S T 2 2')。

[数223]

$$\begin{aligned}
C'_{2X} &= Y_j^s, C''_{2X} = Y_j^{rs}, C'_{2Y} = X_j^t, C''_{2Y} = X_j^{rt}, \\
C'_{2Z} &= Y_j^k, C''_{2Z} = Y_j^{rk}, C'_{2Z1} = X_j^k, C''_{2Z1} = X_j^{rk}, \\
C_3 &= e(g_2 g_4, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r, \\
C_{5X} &= (g_4 \cdot g^y)^{\frac{1}{s}}, C_{5Y} = (g_2 \cdot g^y)^{\frac{1}{t}}, C_{5Z} = (g_4 \cdot g_2 \cdot g^y)^{\frac{1}{k}}.
\end{aligned}$$

[0861] ステップS T 2 2' の終了後、暗号文生成部 2 4 は、ステップS T 2 3 と同様に、使い捨て署名 σ を生成する。

[0862] しかる後、暗号文生成部 2 4 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 $C_j = (C_1, C_{2X}, C_{2X}', C_{2Y}, C_{2Y}', C_{2Z}, C_{2Z}', C_{2Z1}, C_{2Z1}', C_{5X}, C_{5Y}, C_{5Z}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部 2 1 に書き込む。

[0863] 通信部 2 2 は、制御部 2 5 に制御されて一時データ記憶部 2 1 内の暗号文データ C_j を復号装置 5 0 に送信する。

[0864] 復号装置 5 0 は、暗号化装置 2 0 において生成された暗号文データ C_j をステップS T 5 1 と同様に検証する。検証が成功した場合、復号装置 5 0 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224]

【数224】

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

[0865] 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、 $g_1 = g^\alpha$, $g_2 = g^\beta$, $g_3 = g^\xi$, $g_4 = g^{\alpha\xi}$ と書き替えて表記している。

[数225]

$$\begin{aligned}
 & \frac{C_3}{\left\{ \left(\frac{e(C_{5Z}, C''_{2Z})}{e(C_{5X}, C''_{2X})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C''_{2Z1})}{e(C_{5Y}, C''_{2Y})} \right)^{\frac{1}{x_j}} \right\}} \\
 &= \frac{C_3}{\left\{ \left(\frac{e(g^{\frac{\alpha\xi+\beta+\gamma}{k}}, g^{y_jrk})}{e(g^{\frac{\alpha\xi+\gamma}{s}}, g^{y_jrs})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\alpha\xi+\beta+\gamma}{k}}, g^{x_jrk})}{e(g^{\frac{\beta+\gamma}{t}}, g^{x_jrt})} \right)^{\frac{1}{x_j}} \right\}} \\
 &= \frac{C_3}{\left\{ \left(\frac{e(g^{(\alpha\xi+\beta+\gamma)y_jr}, g)}{e(g^{(\alpha\xi+\gamma)y_jr}, g)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(\alpha\xi+\beta+\gamma)x_jr}, g)}{e(g^{(\beta+\gamma)x_jr}, g)} \right)^{\frac{1}{x_j}} \right\}} \\
 &= \frac{m \cdot e(g_2 g_4, g)^r}{(e(g, g)^{\beta r} \cdot e(g, g)^{\alpha\xi r})} = m
 \end{aligned}$$

[0866] [変形例28]

第13の実施形態では、公開パラメータにシステム固定値の5つの元 g , g_1 , g_2 , g_3 , g_4 が含まれる例を説明したが、これに限らず、元 g_2 , g_3 , g_4 を生成せず、公開パラメータに元 g_2 , g_3 , g_4 を含めなくてもよい。この場合、第13の実施形態において、 $g_2 = g$, $g_3 = g$, $g_4 = g$ として、 g_2 , g_3 , g_4 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。

[0867] [変形例29]

第13の実施形態では、公開パラメータにシステム固定値の5つの元 g ,

g_1, g_2, g_3, g_4 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6つ以上の元を含めてもよい。例えば、公開パラメータに6つの元 $g, g_1, g_2, g_3, g_4, g_5$ を含める場合、第13の実施形態において、 $g_2 = g_2 g_5$ として、 g_2 を $g_2 g_5$ に置き換えればよい。

[0868] また、例えば、公開パラメータに7つの元 $g, g_1, g_2, g_3, g_4, g_5, g_6$ を含める場合、第13の実施形態において、 $g_1 = g_1 g_5, g_2 = g_2 g_6, g_4 = g_4 g_5$ として、 g_1 を $g_1 g_5$ に、 g_2 を $g_2 g_6$ に、 g_4 を $g_4 g_5$ 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。

[0869] (第14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。鍵セットアップ処理、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アップ処理、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、上述した第13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。

[0870] (1) 鍵セットアップ処理

公開パラメータは、第13の実施形態と同じである。鍵生成部14は、再暗号化鍵生成装置30の識別情報を i 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 $sk_i = (x_i, y_i, z_i, w_i)$ を用いて再暗号化鍵生成装置30の暗号化用公開鍵

[数226]

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

[0871] を生成する（S T 7）。

[0872] ここで、

[数227]

$$X_i = g^{x_i}, Y_i = g^{y_i}, Y_{1i} = g_1^{y_i}, Z_i = g^{z_i}, Z_{1i} = g_1^{z_i}, W_i = g^{w_i}$$

[0873] である。

[0874] また、この秘密鍵 $s k_i$ を用いて再暗号化鍵生成装置 30 の再暗号化鍵生成用公開情報

[数228]

$$pi_i = (X_{3i}, Y_{2i})$$

[0875] を生成する（S T 7'）。

[0876] ここで、

[数229]

$$X_{3i} = g_3^{x_i}, Y_{2i} = g_2^{y_i}$$

[0877] である。

[0878] また同様に、鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、復号装置 50 の秘密鍵 $s k_j = (x_j, y_j, z_j, w_j)$ を生成し、この秘密鍵 $s k_j$ を用いて復号装置 50 の暗号化用公開鍵

[数230]

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

[0879] を生成する（S T 10）。

[0880] ここで、

[数231]

$$X_j = g^{x_j}, Y_j = g^{y_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, Z_{1j} = g_1^{z_j}, W_j = g^{w_j}$$

[0881] である。

[0882] また、この秘密鍵 $s k_j$ を用いて復号装置 50 の再暗号化鍵生成用公開情報

[数232]

$$pi_j = (X_{3j}, Y_{2j})$$

[0883] を生成する (ST10')。

[0884] ここで、

[数233]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

[0885] である。

[0886] (2) 暗号化処理

第13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、 (ssk, sk_v) を生成し(ST21)、暗号化データ C_1 に検証鍵 sk_v をセットする($C_1 = sk_v$)。

[0887] 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。

[0888] 暗号文生成部24は、この乱数 r 、再暗号化鍵生成装置30の暗号化用公開鍵 pk_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_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 , C_4 を生成する(ST22)。

[数234]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r,$$

$$C_{2F} = F_i(L)^r, C_3 = e(g_2 g_4, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r$$

[0889] ここで、関数 $F_i(L)$ は次式により定義される。

[数235]

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z})$$

[0890] ステップS T 2 2の終了後、暗号文生成部2 4は、時間パラメータL及び暗号化データ C_3 , C_4 に対して、

[数236]

公開パラメータにおける署名生成機能 $\hat{S}$ [0891] とステップS T 2 1で生成した署名鍵 $s s k$ 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 2 3)。

[数237]

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

[0892] しかる後、暗号文生成部2 4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 $C_i = (L, C_1, C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_{2F}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部2 1に書き込む。

[0893] (3) 再暗号化鍵生成処理

乱数生成部3 6は、3つの乱数 $\gamma, \delta_x, \delta_y \in Z_p^*$ を生成して再暗号化鍵生成部3 4に送出する。

[0894] 再暗号化鍵生成部 34 は、これらの乱数 γ , δ_x , δ_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 の再暗号化鍵生成用公開情報 p_{i_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 (S T 32)。

[数238]

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

[0895] ここで、

[数239]

$$R_{ijL1} = (X_{3j} \cdot g^\gamma)^{\frac{1}{x_i}} \cdot F_i(L)^{\delta_x} = g^{\frac{\xi x_j + \gamma}{x_i} + (L + w_i) \delta_x}$$

$$R_{ijL2} = (Y_{2j} \cdot g^\gamma)^{\frac{1}{y_i}} \cdot F_i(L)^{\delta_y} = g^{\frac{\beta y_j + \gamma}{y_i} + (L + w_i) \delta_y}$$

$$R_{ijL3} = (X_{3j} \cdot Y_{2j} \cdot g^\gamma)^{\frac{1}{z_i}} = g^{\frac{\xi x_j + \beta y_j + \gamma}{z_i}}$$

$$R_{ijL4} = (g^{x_i})^{\delta_x} = g^{x_i \delta_x}$$

$$R_{ijL5} = (g^{y_i})^{\delta_y} = g^{y_i \delta_y}$$

[0896] である。なお、上式では、 $g_1 = g^\alpha$, $g_2 = g^\beta$, $g_3 = g^\xi$, $g_4 = g^{\alpha \xi}$ と書き替えて表記している。

[0897] (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 (S T 41)。

[数240]

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

[0898] 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。

[0899] 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 , $h \in \mathbb{Z}_p^*$ を生成して再暗号化処理部44に送出する。

[0900] 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241]

$$\begin{aligned}
C'_{2X} &= X_i^s, C''_{2X} = C_{2X}^s = X_i^{rs}, C'_{2Y} = Y_{1i}^t, C''_{2Y} = C_{2Y}^t = Y_{1i}^{rt}, \\
C'_{2Z} &= Z_i^k, C''_{2Z} = C_{2Z}^k = Z_i^{rk}, C'_{2Z1} = Z_{1i}^k, C''_{2Z1} = C_{2Z1}^k = Z_{1i}^{rk}, \\
C'_{2F} &= F_i(L)^h, C''_{2F} = C_{2F}^h = F_i(L)^{rh}, \\
C_{5X} &= R_{ijL1}^{\frac{1}{s}}, C_{5Y} = R_{ijL2}^{\frac{1}{t}}, C_{5Z} = R_{ijL3}^{\frac{1}{k}}, \\
C_{5FX} &= R_{ijL4}^{\frac{1}{h}}, C_{5FY} = R_{ijL5}^{\frac{1}{h}}
\end{aligned}$$

[0901] ステップS T 4 2の終了後、再暗号化処理部4 4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4 2に書き込む。

[0902] (5) 復号処理

復号処理部5 4は、公開パラメータ及び自装置5 0の暗号化用公開鍵 $p k_j$ と次の検証式を用い、一時データ記憶部5 2内の再暗号文データ C_j を検証する(S T 5 1)。

[数242]

$$\begin{aligned}
e(C_{2X}'', u^{C_1} \cdot v) &= e(C_{2X}', C_4) \\
e(C_{2Y}'', u^{C_1} \cdot v) &= e(C_{2Y}', C_4) \\
e(C_{2Z}'', u^{C_1} \cdot v) &= e(C_{2Z}', C_4) \\
e(C_{2Z1}'', u^{C_1} \cdot v) &= e(C_{2Z1}', C_4) \\
e(C_{2F}'', u^{C_1} \cdot v) &= e(C_{2F}', C_4) \\
e(C_{5Z}, C_{2Z}') \cdot e(C_{5FX}, C_{2F}') &= e(C_{5X}, C_{2X}') \cdot e(Y_j, g_2) \\
e(C_{5Z}, C_{2Z1}') \cdot e(C_{5FY}, C_{2F}') &= e(C_{5Y}, C_{2Y}') \cdot e(X_j, g_4) \\
\hat{V}(C_1, \sigma, (C_3, C_4)) &= 1
\end{aligned}$$

[0903] 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。

[0904] 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243]

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

[0905] 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、 $g_1 = g^\alpha$ 、 $g_2 = g^\beta$ 、 $g_3 = g^\xi$ 、 $g_4 = g^{\alpha\xi}$ と書き替えて表記している。

[数244]

$$\begin{aligned}
& \frac{C_3}{\left\{ \left(\frac{e(C_{SZ}, C_{2Z}^n) \cdot e(C_{SFZ}, C_{2F}^n)}{e(C_{SX}, C_{2X}^n)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{SZ}, C_{2Z}^n) \cdot e(C_{SFF}, C_{2F}^n)}{e(C_{SY}, C_{2Y}^n)} \right)^{\frac{1}{x_j}} \right\}} \\
&= \frac{C_3}{\left\{ \left(\frac{e(g^{\frac{\xi_j + \beta_j + \gamma}{z_k}}, g^{\frac{x_i \delta_x}{h}})^{\frac{1}{y_j}} \cdot e(g^{\frac{\xi_j + \beta_j + \gamma}{z_k}}, g^{\frac{\alpha_j \delta_y}{h}})^{\frac{1}{x_j}} \right)}{e(g^{\frac{\xi_j + \gamma}{x_i} + (L + w_i) \delta_x}, g^{\frac{1}{s}})^{\frac{1}{y_j}} \cdot e(g^{\frac{\beta_j + \gamma}{y_i} + (L + w_i) \delta_y}, g^{\frac{1}{t}})^{\frac{1}{x_j}}} \right\}} \\
&= \frac{C_3}{\left\{ \left(\frac{e(g^{(\xi_j + \beta_j + \gamma)r}, g)}{e(g^{(\xi_j + \gamma)r + (L + w_i) \delta_x r}, g)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(\xi_j + \beta_j + \gamma)\alpha}, g) \cdot e(g^{\alpha_j \delta_y (L + w_i)r}, g)}{e(g^{(\beta_j + \gamma)\alpha + (L + w_i) \delta_y y_i \alpha}, g)} \right)^{\frac{1}{x_j}} \right\}} \\
&= \frac{m \cdot e(g_2 g_4, g)^r}{(e(g, g)^{\beta_r} \cdot e(g, g)^{\alpha \xi_r})} = m
\end{aligned}$$

[0906] 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。

[0907] 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 γ , 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13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。

[0908] [変形例30]

第14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よい。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よい。本変形例における鍵セットアップ処理は、第 14 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。

[0909] 本変形例における暗号化処理と、第 14 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 ($ST24'$)。

[0910] 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245]

$$m = \frac{C_3}{e(g_2 g_4, C_{2X})^{\frac{1}{x_i}}}$$

[0911] 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。

[数246]

$$\begin{aligned}
& \frac{m \cdot e(g_2 g_4, g)^r}{e(g_2 g_4, C_{2X})^{\frac{1}{x_i}}} \\
&= \frac{m \cdot e(g_2 g_4, g)^r}{e(g_2 g_4, g^{x_i r})^{\frac{1}{x_i}}} \\
&= \frac{m \cdot e(g_2 g_4, g)^r}{e(g_2 g_4, g)^r} = m
\end{aligned}$$

[0912] [変形例 3 1]

変形例 3 0 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よい。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よい。本変形例における鍵セットアップ処理、復号処理は、第 1 4 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 5 0 の識別情報を j とする。

[0913] 暗号化装置 2 0 の暗号化パラメータ生成部 2 3 は、ステップ S T 2 1 と同様に $(s s k, s v k)$ を生成し (S T 2 1')、暗号化データ C_1 に検証鍵 $s v k$ をセットする ($C_1 = s v k$)。

[0914] また、暗号化パラメータ生成部 2 3 は、8 つの乱数 $r, s, t, k, h, \gamma, \delta_x, \delta_y \in \mathbb{Z}_p^*$ を生成して暗号文生成部 2 4 に送出する。

[0915] 暗号文生成部 2 4 は、これらの乱数 $r, s, t, k, h, \gamma, \delta_x, \delta_y$ 、復号装置 5 0 の暗号化用公開鍵 $p k_j$ 、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 (S T 2 2')。

[数247]

$$\begin{aligned} C_{2X}' &= Y_j^s, C_{2X}'' = Y_j^{rs}, C_{2Y}' = X_j^t, C_{2Y}'' = X_j^{rt}, \\ C_{2Z}' &= Y_j^k, C_{2Z}'' = Y_j^{rk}, C_{2Z1}' = X_j^k, C_{2Z1}'' = X_j^{rk}, \\ C_{2F}' &= F_j(L)^h, C_{2F}'' = F_j(L)^{rh}, \\ C_3 &= e(g_2 g_4, g)^r \cdot m, C_4 = (u^{svk} \cdot v)^r, \\ C_{5X} &= (g_4 \cdot g^\gamma \cdot F_j(L)^{\delta_y})^{\frac{1}{s}} = g^{\frac{\alpha\xi + \gamma + (L+w_j)\delta_y}{s}}, \\ C_{5Y} &= (g_2 \cdot g^\gamma \cdot F_j(L)^{\delta_x})^{\frac{1}{t}} = g^{\frac{\beta + \gamma + (L+w_j)\delta_x}{t}}, \\ C_{5Z} &= (g_4 \cdot g_2 \cdot g^\gamma)^{\frac{1}{k}} = g^{\frac{\alpha\xi + \beta + \gamma}{k}}, \\ C_{5FX} &= Y_j^{\frac{\delta_y}{h}}, C_{5FY} = X_j^{\frac{\delta_x}{h}} \end{aligned}$$

[0916] ステップS T 2 2' の終了後、暗号文生成部24は、ステップS T 2 3と同様に、使い捨て署名 σ を生成する。

[0917] 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。

[0918] 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。

[0919] 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248]

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

[0920] 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、 $g_1 = g^\alpha$, $g_2 = g^\beta$, $g_3 = g^\xi$, $g_4 = g^{\alpha\xi}$ と書き替えて表記している。

[数249]

$$\begin{aligned} & \frac{C_3}{\left\{ \left(\frac{e(C_{5Z}, C_{2Z}^{\prime\prime}) \cdot e(C_{5FX}, C_{2F}^{\prime\prime})}{e(C_{5X}, C_{2X}^{\prime\prime})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(C_{5Z}, C_{2Z1}^{\prime\prime}) \cdot e(C_{5FY}, C_{2F}^{\prime\prime})}{e(C_{5Y}, C_{2Y}^{\prime\prime})} \right)^{\frac{1}{x_j}} \right\}} \\ &= \frac{C_3}{\left\{ \left(\frac{e(g^{\frac{\alpha\xi+\beta+\gamma}{k}}, g^{y_j r^k}) \cdot e(g^{\frac{y_j \delta_y}{h}}, g^{(L+w_j) r h})}{e(g^{\frac{\alpha\xi+\gamma+(L+w_j)\delta_y}{s}}, g^{y_j r^s})} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{\frac{\alpha\xi+\beta+\gamma}{k}}, g^{x_j r^k}) \cdot e(g^{\frac{x_j \delta_x}{h}}, g^{(L+w_j) r h})}{e(g^{\frac{\beta+\gamma+(L+w_j)\delta_x}{t}}, g^{x_j r^t})} \right)^{\frac{1}{x_j}} \right\}} \\ &= \frac{C_3}{\left\{ \left(\frac{e(g^{(\alpha\xi+\beta+\gamma)r_j}, g) \cdot e(g^{y_j \delta_y (L+w_j) r}, g)}{e(g^{(\alpha\xi+\gamma)y_j r + (L+w_j)\delta_y y_j r}, g)} \right)^{\frac{1}{y_j}} \cdot \left(\frac{e(g^{(\alpha\xi+\beta+\gamma)x_j r}, g) \cdot e(g^{x_j \delta_x (L+w_j) r}, g)}{e(g^{(\beta+\gamma)x_j r + (L+w_j)\delta_x x_j r}, g)} \right)^{\frac{1}{x_j}} \right\}} \\ &= \frac{m \cdot e(g_2 g_4, g)^r}{(e(g, g)^{\beta r} \cdot e(g, g)^{\alpha \xi r})} = m \end{aligned}$$

[0921] 以上で説明した第 13 及び第 14 の実施形態のうちの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。

[0922] また、本来の委譲先の再暗号化鍵生成用公開情報を用いて再暗号化鍵を生成する構成により、当該委譲先が再暗号化鍵生成用公開情報を提供しなければ再暗号化鍵は生成できない。そのため、本来の委譲先の許可の下であれば、再暗号化鍵を生成することができるようになる。

[0923] 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。

[0924] 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。

[0925] 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。

[0926] 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。

[0927] 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。

[0928] 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。

[0929] 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。

[0930] 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公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵を記憶する第2記憶手段（32）と、

前記第1秘密鍵及び前記第2再暗号化鍵生成鍵に基づいて、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、

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3] 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 $s k_i = (x_i, y_i, z_i)$ で表し、前記第2秘密鍵を $s k_j = (x_j, y_j, z_j)$ 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、 $g, g_1, g_2 \in G$ ）、前記第1公開鍵を $p k_i$ で表すとき、前記第1公開鍵 $p k_i$ は、データ X_i, Y_{1i}, Z_i, Z_{1i} を含んでおり（但し、

[数1]

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

)、

前記第2公開鍵を $p k_j$ で表すとき、前記第2公開鍵 $p k_j$ は、データ X_j , Y_{1j} , Z_j , Z_{1j} を含んでおり（但し、

[数2]

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

）、

前記第2再暗号化鍵生成鍵に関する乱数を π で表し、前記乱数 π と前記システム固定値 g に基づく値を g_3 で表し、前記乱数 π と前記システム固定値 g_1 に基づく値を g_4 で表し、前記乱数 π と前記システム固定値 g_2 に基づく値を g_5 で表し（但し、 $g_3 = g^\pi$, $g_4 = g_1^\pi$, $g_5 = g_2^\pi$ ）、前記第2再暗号化鍵生成鍵を $r k_j$ で表すとき、

$$r k_j = (X_{3j}, Y_{5j})$$

であり（但し、

[数3]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

）、

前記平文データを m で表し（但し、 $m \in G_T$ ）、前記暗号文データに関する乱数を 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）、前記暗号文データ C_i は、データ C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_3 を含んでおり（但し、

[数4]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_5, g)^r \cdot m$$

）、

前記再暗号化鍵に関する乱数を θ で表し、前記システム固定値 g 、 g_2 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、

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

であり（但し、

[数5]

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}.$$

）、

前記再暗号文データを C_j で表すとき（但し、3つの乱数を s 、 t 、 k で表す）、前記再暗号文データ C_j は、データ $C_{2X}^{''}$ 、 $C_{2Y}^{''}$ 、 $C_{2Z}^{''}$ 、 $C_{2Z1}^{''}$ 、 C_{5X} 、 C_{5Y} 、 C_{5Z} 、 C_3 を含んでおり（但し、

[数6]

$$C_{2X}'' = C_{2X}^s = X_i^{rs}, \quad C_{2Y}'' = C_{2Y}^t = Y_{1i}^{rt},$$

$$C_{2Z}'' = C_{2Z}^k = Z_i^{rk}, \quad C_{2Z1}'' = C_{2Z1}^k = Z_{1i}^{rk},$$

$$C_{5X} = R_{ij1}^{\frac{1}{s}}, \quad C_{5Y} = R_{ij2}^{\frac{1}{t}}, \quad C_{5Z} = R_{ij3}^{\frac{1}{k}}$$

),

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、

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

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 $s k_i = (x_i, y_i, z_i, w_i)$ で表し、前記第2秘密鍵を $s k_j = (x_j, y_j, z_j, w_j)$ 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、 $g, g_1, g_2 \in G$ ）、前記第1公開鍵を $p k_i$ で表すとき、前記第1公開鍵 $p k_i$ は、データ $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ を含んでおり（但し、

[数7]

$$X_i = g^{x_i}, \quad Y_{1i} = g_1^{y_i}, \quad Z_i = g^{z_i},$$

$$Z_{1i} = g_1^{z_i}, \quad W_i = g^{w_i}$$

),

前記第2公開鍵を $p k_j$ で表すとき、前記第2公開鍵 $p k_j$ は、データ $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$ を含んでおり（但し、

[数8]

$$X_j = g^{X_j}, Y_{1j} = g_1^{Y_j}, Z_j = g^{Z_j}, \\ Z_{1j} = g_1^{Z_j}, W_j = g^{W_j}$$

)、

前記第2再暗号化鍵生成鍵に関する乱数を π で表し、前記乱数 π と前記システム固定値 g に基づく値を g_3 で表し、前記乱数 π と前記システム固定値 g_1 に基づく値を g_4 で表し、前記乱数 π と前記システム固定値 g_2 に基づく値を g_5 で表し（但し、 $g_3 = g^\pi$, $g_4 = g_1^\pi$, $g_5 = g_2^\pi$ ）、前記第2再暗号化鍵生成鍵を r_{k_j} で表すとき、

$$r_{k_j} = (X_{3j}, Y_{5j})$$

であり（但し、

[数9]

$$X_{3j} = g_3^{X_j}, Y_{5j} = g_5^{Y_j}$$

)、

前記平文データを m で表し（但し、 $m \in G_T$ ）、前記暗号文データに関する乱数を r で表し、前記位数 p に対する乗法群を Z_p^* で表し、前記再暗号化鍵を更新する期間を示す時間パラメータを L 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）、前記暗号文データ C_i は、データ C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 を含んでおり（但し、

[数10]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_{2F} = F_i(L)^r, C_3 = e(g_4 g_5, g)^r \cdot m$$

ここで、

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

)、

前記再暗号化鍵に関する3つの乱数を θ , δ_x , δ_y で表し、前記システム固定値 g , g_1 に関するべき指数を α で表し、前記システム固定値 g , g_2 に関するべき指数を β で表し（但し、 $g_1 = g^\alpha$, $g_2 = g^\beta$ ）、前記再暗号化鍵を R_{ijL} で表すとき、

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

であり（但し、

[数11]

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i \delta_x}, R_{ijL5} = g_1^{y_i \delta_y} = g^{\alpha y_i \delta_y}$$

)、

前記再暗号文データを C_j で表すとき（但し、4つの乱数を s , t

、 k 、 h で表す)、前記再暗号文データ C_j は、データ $C_{2X}^{''}$ 、 $C_{2Y}^{''}$ 、 $C_{2Z}^{''}$ 、 $C_{2Z1}^{''}$ 、 $C_{2F}^{''}$ 、 C_{5X} 、 C_{5Y} 、 C_{5Z} 、 C_{5FX} 、 C_{5FY} 、 C_3 を含んでおり(但し、

[数12]

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

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, \quad C_{5Y} = R_{ijL2}^{\frac{1}{t}}, \quad C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, \quad C_{5FY} = R_{ijL5}^{\frac{1}{h}},$$

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 の関係は、

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

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鍵により再暗号化して、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るための再暗号化装置(40)であって、

予め再暗号化鍵生成装置により生成された前記再暗号化鍵を記憶する記憶手段(41)と、

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得る再暗号化手段(44)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、及び前

記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵に基づいて、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]

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鍵により再暗号化して、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装置に対し、前記暗号文データを生成する暗号化装置(20)であって、

前記第1公開鍵を記憶する記憶手段(21)と、

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取得する暗号化手段(24)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、及び前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵に基づいて、生成されていることを特徴とする暗号化装置。

[請求項7]

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取得後に、前記再暗号文データを復号する復号装置(50)であって、

前記第2秘密鍵を記憶する記憶手段(51)と、

前記記憶手段内の第2秘密鍵に基づいて、前記再暗号文データを復号して前記平文データを取得する復号手段(54)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、及び前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵に基づいて、生成されていることを特徴とする

復号装置。

[請求項8]

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(33)を前記プロセッサに実行させる第1プログラムコードと、

前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成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(33)を前記プロセッサに実行させる第2プログラムコードと、

前記第1秘密鍵及び前記第2再暗号化鍵生成鍵に基づいて、前記再暗号化鍵を生成する処理(34)を前記プロセッサに実行させる第3プログラムコードと、

を備えたプログラム。

[請求項9]

請求項8に記載のプログラムにおいて、

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プログラム。

[請求項10]

請求項9に記載のプログラムにおいて、

前記第1秘密鍵を $s k_i = (x_i, y_i, z_i)$ で表し、前記第2秘密鍵を $s k_j = (x_j, y_j, z_j)$ 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

$_2 \in G$)、前記第1公開鍵を $p k_i$ で表すとき、前記第1公開鍵 $p k_i$ は、データ X_i, Y_{1i}, Z_i, Z_{1i} を含んでおり（但し、

[数13]

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

)、

前記第2公開鍵を $p k_j$ で表すとき、前記第2公開鍵 $p k_j$ は、データ X_j, Y_{1j}, Z_j, Z_{1j} を含んでおり（但し、

[数14]

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

)、

前記第2再暗号化鍵生成鍵に関する乱数を π で表し、前記乱数 π と前記システム固定値 g に基づく値を g_3 で表し、前記乱数 π と前記システム固定値 g_1 に基づく値を g_4 で表し、前記乱数 π と前記システム固定値 g_2 に基づく値を g_5 で表し（但し、 $g_3 = g^\pi$, $g_4 = g_1^\pi$, $g_5 = g_2^\pi$ ）、前記第2再暗号化鍵生成鍵を $r k_j$ で表すとき、

$$r k_j = (X_{3j}, Y_{5j})$$

であり（但し、

[数15]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

)、

前記平文データを m で表し（但し、 $m \in G_T$ ）、前記暗号文データに関する乱数を 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）、前記暗号文データ C_i は、データ $C_{2X}, C_{2Y}, C_{2Z}, C_{2Z1}, C_3$ を含んでおり（但し

、

[数16]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_3 = e(g_4 g_5, g)^r \cdot m.$$

)、

前記再暗号化鍵に関する乱数を θ で表し、前記システム固定値 g 、 g_2 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、

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

であり（但し、

[数17]

$$R_{ij1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} = g^{\frac{\pi(x_j + \theta)}{x_i}},$$

$$R_{ij2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} = g^{\frac{\pi(\beta y_j + \theta)}{y_i}},$$

$$R_{ij3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j + \beta y_j + \theta)}{z_i}}.$$

)、

前記再暗号文データを C_j で表すとき（但し、3つの乱数を s 、 t 、 k で表す）、前記再暗号文データ C_j は、データ $C_{2X}^{s'}$ 、 $C_{2Y}^{t'}$ 、 $C_{2Z}^{k'}$ 、 $C_{2Z1}^{s'}$ 、 C_{5X} 、 C_{5Y} 、 C_{5Z} 、 C_3 を含んでおり（但し、

[数18]

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

)、

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、

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

で表されるプログラム。

[請求項11]

請求項9に記載のプログラムにおいて、

前記第1秘密鍵を $s_{k_i} = (x_i, y_i, z_i, w_i)$ で表し、前記第2秘密鍵を $s_{k_j} = (x_j, y_j, z_j, w_j)$ 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、 $g, g_1, g_2 \in G$ ）、前記第1公開鍵を p_{k_i} で表すとき、前記第1公開鍵 p_{k_i} は、データ $X_i, Y_{1i}, Z_i, Z_{1i}, W_i$ を含んでおり（但し、

[数19]

$$\begin{aligned}
X_i &= g^{x_i}, \quad Y_{1i} = g_1^{y_i}, \quad Z_i = g^{z_i}, \\
Z_{1i} &= g_1^{z_i}, \quad W_i = g^{w_i}
\end{aligned}$$

)、

前記第2公開鍵を p_{k_j} で表すとき、前記第2公開鍵 p_{k_j} は、データ $X_j, Y_{1j}, Z_j, Z_{1j}, W_j$ を含んでおり（但し、

[数20]

$$X_j = g^{x_j}, Y_{1j} = g_1^{y_j}, Z_j = g^{z_j}, \\ Z_{1j} = g_1^{z_j}, W_j = g^{w_j}$$

)、

前記第2再暗号化鍵生成鍵に関する乱数を π で表し、前記乱数 π と前記システム固定値 g に基づく値を g_3 で表し、前記乱数 π と前記システム固定値 g_1 に基づく値を g_4 で表し、前記乱数 π と前記システム固定値 g_2 に基づく値を g_5 で表し（但し、 $g_3 = g^\pi$, $g_4 = g_1^\pi$, $g_5 = g_2^\pi$ ）、前記第2再暗号化鍵生成鍵を r_{kj} で表すとき、

$$r_{kj} = (X_{3j}, Y_{5j})$$

であり（但し、

[数21]

$$X_{3j} = g_3^{x_j}, Y_{5j} = g_5^{y_j}$$

)、

前記平文データを m で表し（但し、 $m \in G_T$ ）、前記暗号文データに関する乱数を r で表し、前記位数 p に対する乗法群を Z_p^* で表し、前記再暗号化鍵を更新する期間を示す時間パラメータを L 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）、前記暗号文データ C_i は、データ C_{2X} , C_{2Y} , C_{2Z} , C_{2Z1} , C_{2F} , C_3 を含んでおり（但し、

[数22]

$$C_{2X} = X_i^r, C_{2Y} = Y_{1i}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{1i}^r, \\ C_{2F} = F_i(L)^r, C_3 = e(g_4 g_5, g)^r \cdot m,$$

ここで、

$$F_i(L) = g^L \cdot W_i = g^{L+w_i} \quad (L \in \mathbb{Z}_p^*)$$

)、

前記再暗号化鍵に関する3つの乱数を θ , δ_x , δ_y で表し、前記システム固定値 g , g_1 に関する2つのベキ指数を α で表し、前記システム固定値 g , g_2 に関するベキ指数を β で表し（但し、 $g_1 = g^\alpha$, $g_2 = g^\beta$ ）、前記再暗号化鍵を R_{ijL} で表すとき、

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

であり（但し、

[数23]

$$R_{ijL1} = (X_{3j} \cdot g_3^\theta)^{1/x_i} \cdot g^{(L+w_i)\delta_x} = g^{\frac{\pi(x_j+\theta)}{x_i} + (L+w_i)\delta_x},$$

$$R_{ijL2} = (Y_{5j} \cdot g_3^\theta)^{1/y_i} \cdot g^{(L+w_i)\delta_y} = g^{\frac{\pi(\beta y_j+\theta)}{y_i} + (L+w_i)\delta_y},$$

$$R_{ijL3} = (X_{3j} \cdot Y_{5j} \cdot g_3^\theta)^{1/z_i} = g^{\frac{\pi(x_j+\beta y_j+\theta)}{z_i}},$$

$$R_{ijL4} = g^{x_i \delta_x}, R_{ijL5} = g_1^{y_i \delta_y} = g^{\alpha y_i \delta_y}$$

)、

前記再暗号文データを C_j で表すとき（但し、4つの乱数を s , t

、 k 、 h で表す)、前記再暗号文データ C_j は、データ $C_{2X}^{''}$ 、 $C_{2Y}^{''}$ 、 $C_{2Z}^{''}$ 、 $C_{2Z1}^{''}$ 、 $C_{2F}^{''}$ 、 C_{5X} 、 C_{5Y} 、 C_{5Z} 、 C_{5FX} 、 C_{5FY} 、 C_3 を含んでおり(但し、

[数24]

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

$$C_{5X} = R_{ijL1}^{\frac{1}{s}}, \quad C_{5Y} = R_{ijL2}^{\frac{1}{t}}, \quad C_{5Z} = R_{ijL3}^{\frac{1}{k}},$$

$$C_{5FX} = R_{ijL4}^{\frac{1}{h}}, \quad C_{5FY} = R_{ijL5}^{\frac{1}{h}},$$

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_{kj} の関係は、

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

で表されるプログラム。

[請求項12]

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鍵により再暗号化して、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るための再暗号化装置(40)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(M4)に記憶されたプログラムであって、

予め再暗号化鍵生成装置により生成された前記再暗号化鍵を前記再暗号化装置の記憶手段(41)に書込む処理(43)を前記プロセッサに実行させる第1プログラムコードと、

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得る処理(44)を前記プロセ

ッサに実行させる第2プログラムコードと、
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、及び前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵に基づいて、生成されているプログラム。

[請求項13]

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鍵により再暗号化して、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装置(40)に対し、前記暗号文データを生成する暗号化装置(20)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(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)に書込む処理(22)を前記プロセッサに実行させる第1プログラムコードと、

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取得する処理(24)を前記プロセッサに実行させる第2プログラムコードと、

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、及び前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵に基づいて、生成されているプログラム。

[請求項14]

再暗号化装置(40)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取得後に、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(53)を前記プロセッサに実行させる第1プログラムコードと、

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

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、及び前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵に基づいて、生成されているプログラム。

[請求項15]

第1ユーザ装置の暗号化用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、

前記暗号化用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秘密鍵に対応する再暗号化鍵生成用公開情報を記憶する第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、前記再暗号化鍵生成用公開情報及び前記第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16]

請求項15に記載の再暗号化鍵生成装置において、

前記再暗号化鍵生成手段は、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、前記再暗号化鍵生成用公開情報及び前記第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17]

請求項15に記載の再暗号化鍵生成装置において、

前記暗号化用公開鍵は、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、

前記再暗号化鍵生成用公開情報は、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18]

請求項16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 $s k_i = (x_i, y_i, z_i)$ で表し、前記第2秘密鍵を $s k_j = (x_j, y_j, z_j)$ で表し、前記第1乱数を γ で表し、前記複数のシステム固定値を g, g_1, g_2, g_3, g_4 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、 $g, g_1, g_2, g_3, g_4 \in G$ ）、前記各システム固定値に関するベキ指数を α, β, ξ で表し（但し、 $g_1 = g^\alpha, g_2 = g^\beta, g_3 = g^\xi, g_4 = g^{\alpha\xi}$ ）、前記再暗号化鍵を R_{ij} で表すとき、

[数25]

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

であり（但し、

[数26]

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

）、

前記第1ユーザ装置の暗号化用公開鍵を $p k_i$ で表すとき、

[数27]

$$p k_i = (X_i, Y_{1i}, Z_i, Z_{1i})$$

であり（但し、

[数28]

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

)、

前記第1秘密鍵に対応する再暗号化鍵生成用公開情報を pi_i で表すとき、

[数29]

$$pi_i = (X_{3i}, Y_{2i})$$

であり（但し、

[数30]

$$X_{3i} = g^{x_i}, Y_{2i} = g_2^{y_i}$$

)、

前記第2ユーザ装置の暗号化用公開鍵を pk_j で表すとき、

[数31]

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

であり（但し、

[数32]

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

)、

前記第2秘密鍵に対応する再暗号化鍵生成用公開情報を pi_j で表すとき、

[数33]

$$pi_j = (X_{3j}, Y_{2j})$$

であり（但し、

[数34]

$$X_{3j} = g_3^{x_j}, Y_{2j} = g_2^{y_j}$$

）、

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 $e(g, h)$ （但し、 $g, h \in G$ ）で表す）、

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

であり（但し、

[数35]

$$C_{2X} = X_i^r, C_{2Y} = Y_{li}^r, C_{2Z} = Z_i^r, C_{2Z1} = Z_{li}^r, C_3 = e(g_2 g_4, g)^r \cdot m$$

）、

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36]

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

)、

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、

[数37]

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

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19]

第 1 ユーザ装置の暗号化用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

得る再暗号化手段（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、前記暗号化用公開鍵に対応する第１秘密鍵、前記第２秘密鍵に対応する再暗号化鍵生成用公開情報、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20] 請求項１９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21] 第１ユーザ装置の暗号化用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、

前記暗号化用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プログラムコードと、

前記第２秘密鍵に対応する再暗号化鍵生成用公開情報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プログラムコードと、

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

前記第１秘密鍵、前記再暗号化鍵生成用公開情報及び前記第１乱数に基づいて、前記再暗号化鍵を生成する処理（３４）を前記プロセッサに実行させる第４プログラムコードと、

を備えたプログラム。

[請求項22]

請求項 2 1 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23]

第 1 ユーザ装置の暗号化用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るための再暗号化鍵を生成する再暗号化鍵生成装置 (3 0) に通信可能な再暗号化装置 (4 0) 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 (4 1) 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得る処理 (4 4) を前記プロセッサに実行させる第 2 プログラムコードと、

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処理 (4 3) を前記プロセッサに実行させる第 3 プログラムコードと、

を備え、

前記再暗号化鍵は、前記暗号化用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 再暗号化鍵生成用公開情報、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、生成されているプログラム。

[請求項24]

第 1 ユーザ装置の暗号化用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るための再暗号化鍵を

用いる再暗号化装置（４０）に通信可能な暗号化装置（２０）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（Ｍ２）に記憶されたプログラムであって、

前記暗号化用公開鍵を前記暗号化装置の記憶手段（２１）に書込む処理（２２）を前記プロセッサに実行させる第１プログラムコードと、

前記記憶手段内の暗号化用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得る処理（２４）を前記プロセッサに実行させる第２プログラムコードと、

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（２２）を前記プロセッサに実行させる第３プログラムコードと、
を備え、

前記再暗号化鍵は、前記暗号化用公開鍵に対応する第１秘密鍵、前記第２秘密鍵に対応する再暗号化鍵生成用公開情報、及び当該再暗号化鍵を生成する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、生成されているプログラム。

[請求項25]

再暗号化装置（４０）が再暗号化鍵に基づいて、第１ユーザ装置の暗号化用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（５３）を前記プロセッサに実行させる第１プログラムコード、

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（５４）を前記プロセッサに実行させる第２プロ

グラムコード、

を備え、

前記再暗号化鍵は、前記暗号化用公開鍵に対応する第1秘密鍵、前記第2秘密鍵に対応する再暗号化鍵生成用公開情報、及び当該再暗号化鍵を生成する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、生成されているプログラム。

[請求項26]

請求項23乃至請求項25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。