

明 細 書

発明の名称：サーバ装置及びプログラム

技術分野

[0001] 本発明の実施形態は、サーバ装置及びプログラムに関する。

背景技術

[0002] ユーザがサーバ装置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、サーバ装置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が挙げられる。

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

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

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

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

[0007] (1)の個別鍵方式では、ユーザ毎に異なる秘密鍵と公開鍵の組を各ユーザがそれぞれ持つ。ユーザAは、(ユーザB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装置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装置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。

[0008] (2)の共通鍵方式では、各ユーザに共通の秘密鍵と公開鍵の組を各ユーザが共有する。ユーザAは、(各ユーザに共通の暗号化鍵である)公開鍵でファイルを暗号化し、暗号化されたファイルをサーバ装置へアップロードする。各ユーザは、同一の秘密鍵を共有している。

[0009] (3)のプロキシ再暗号化方式では、(1)の個別鍵方式と同様に、ユー

ザ毎に異なる秘密鍵と公開鍵の組を各ユーザがそれぞれ持つ。しかしながら、（１）の個別鍵方式とは異なり、ユーザＡは、ユーザのグループを管理するエンティティ（以下、グループ管理者と呼ぶ）の公開鍵（以下、グループ公開鍵と呼ぶ）でファイルを暗号化すれば良く、サーバ装置が、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。

[0010] （１）の個別鍵方式では、新たにユーザＤともファイルを共有したいとき、ユーザＡが（ユーザＤ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装置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）の個別鍵方式は、新規ユーザ数が多かったり、共有したいファイル数が多かったりする場合、新規ユーザ追加時の処理が煩雑となるため、上記ファイル共有システムに不適である。

[0011] （２）の共通鍵方式では、ある時点から（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）復号可能となってしまう不都合がある。このため、（２）の共通鍵方式は、ファイル共有システムに不適である。

[0012] 一方、（３）のプロキシ再暗号化方式では、サーバ装置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。

先行技術文献

非特許文献

[0013] 非特許文献１：B. Libert and D. Vergnaud, "Unidirectional Chosen-Cipher

text Secure Proxy Re-encryption,” Proc. PKC 2008, LNCS 4939, pp.360-379, Springer, 2008.

非特許文献2：G. Ateniese, K. Fu, M. Green and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” Internet Society (ISOC): NDSS 2005, pp. 29-43, 2005.

発明の概要

発明が解決しようとする課題

[0014] しかしながら、(3)のプロキシ再暗号化方式では、ユーザが第三者の提供するファイル共有サービスを利用する場合（例えば、ユーザがインターネットを経由してサーバ装置にアクセスしてサービスを利用する場合）、ユーザがサーバ装置を過度に信頼できないことから、ユーザの秘密鍵をユーザ自身が生成して当該ユーザのみが保持することが望ましい。

[0015] これに対し、(3)のプロキシ再暗号化方式では、再暗号化鍵の更新にグループ公開鍵に対応する秘密鍵（以下、グループ秘密鍵と呼ぶ）を必要とするため、ユーザの秘密鍵をグループ管理者に知らせない場合、グループ秘密鍵を持つグループ管理者が不在の場合に再暗号化鍵を更新できないという不都合がある。

[0016] 本発明が解決しようとする課題は、ユーザの秘密鍵をグループ管理者に知らせない場合、かつグループ管理者が不在の場合でも、再暗号化鍵を更新し得るサーバ装置及びプログラムを提供することである。

課題を解決するための手段

[0017] 実施形態のサーバ装置は、管理者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、ユーザ装置のユーザ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記憶する。

[0018] 前記サーバ装置は、記憶手段、第1計算手段、送受信手段及び第2計算手段を備えている。

[0019] 前記記憶手段は、前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を

記憶する。

[0020] 前記第1計算手段は、前記ユーザ装置から前記再暗号化鍵を更新する旨の通知を受けると、乱数を生成し、前記記憶された再暗号化鍵及び前記生成した乱数に基づいて再暗号化鍵情報を計算する。

[0021] 前記送受信手段は、前記再暗号化鍵情報を前記ユーザ装置に送信し、前記ユーザ装置から更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて当該再暗号化鍵情報から計算された再暗号化鍵更新情報を受信する。

[0022] 前記第2計算手段は、前記再暗号化鍵更新情報及び前記乱数に基づいて前記更新後の再暗号化鍵を計算すると共に、前記記憶手段内の再暗号化鍵を前記更新後の再暗号化鍵に置換する。

図面の簡単な説明

[0023] [図1]図1は、第1の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2]図2は、同実施形態におけるファイル共有システムの概要を示す模式図である。

[図3]図3は、同実施形態におけるファイル共有システムに適用されるサーバ装置、ユーザ装置及びグループ管理者装置の構成を説明するための模式図である。

[図4]図4は、同実施形態における再暗号化鍵の更新処理の概要を示す模式図である。

[図5]図5は、同実施形態における再暗号化鍵の更新処理の動作を説明するためのフローチャートである。

[図6]図6は、同実施形態における再暗号化鍵の更新処理の動作を説明するためのフローチャートである。

[図7]図7は、第3の実施形態における再暗号化鍵の更新処理の概要を示す模式図である。

[図8]図8は、第4の実施形態における再暗号化鍵の更新処理の概要を示す模式図である。

発明を実施するための形態

[0024] 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及び図3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）M1～M4からコンピュータにインストールされ、当該コンピュータのプロセッサに実行されることにより、当該コンピュータに各装置の機能を実現させるためのプログラムが用いられる。

[0025] （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。

[0026] （鍵生成） $\text{KeyGen}(1^k) \rightarrow (p_k, s_k)$

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

[0027] （暗号化） $\text{Enc}(p_{k_A}, m) \rightarrow C_A$

暗号化アルゴリズムEncは、ユーザAの公開鍵 p_{k_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。

[0028] （復号） $\text{Dec}(s_{k_A}, C_A) \rightarrow m$

復号アルゴリズムDecは、ユーザAの秘密鍵 s_{k_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。

[0029] （再暗号化鍵生成） $\text{ReKeyGen}(p_{k_A}, s_{k_A}, p_{k_B}, s_{k_B}) \rightarrow r_{k_{A \rightarrow B}}$

再暗号化鍵生成アルゴリズムReKeyGenは、ユーザAの公開鍵 p_{k_A} 、ユーザAの秘密鍵 s_{k_A} 、ユーザBの公開鍵 p_{k_B} 、ユーザBの秘密鍵 s_{k_B} が入力されると、再暗号化鍵 $r_{k_{A \rightarrow B}}$ を出力する。

[0030] （再暗号化） $\text{ReEnc}(r_{k_{A \rightarrow B}}, C_A) \rightarrow C_B$

再暗号化アルゴリズムReEncは、再暗号化鍵 $r k_{A \rightarrow B}$ 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。

[0031] 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。

[0032] 例えば、再暗号化鍵生成アルゴリズムの入力において、ユーザBの秘密鍵 $s k_B$ を不要とした非相互作用的 (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。

[0033] 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。

[0034] 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。

[0035] 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1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装置 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（以下、ユーザと略記する場合もある） $A, B, C, \dots$ と、ユーザ管理者装置（以下、ユーザ管理者と略記する場合もある） U と、グループ管理者装置（以下、グループ管理者と略記する場合もある） M とを備え、これらが通信網を介して接続されている。通信網とは、例えば、無線LAN (Local Area Network)、有線LAN、光回線網、電話回線網、イントラネット、イーサネット（登録商標）及びインターネットやこれらの組み合わせである。尚、同図では、ファイル共有シ

ステムに接続されるサーバ装置 S_v 及びユーザ装置 $A, B, C, \dots$ は各々 1 台及び 3 台のみ示されているが、これらは各々任意の複数台であっても良い。

[0036] 図 2 は、ファイル共有システムの概要を示す模式図である。このファイル共有システムは、サーバ装置 S_v 、ユーザ A 、ユーザ B 、ユーザ C 、グループ管理者 M 、及びユーザ管理者 U からなる。ユーザ管理者 U 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 U は、ユーザ装置 $A, B, C, \dots$ 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装置 $A, B, C, \dots$ の各ユーザに対して発行する。

[0037] 事前準備として、各ユーザ $A, B, C, \dots$ は、グループ管理者の公開鍵 $p_{k_{Gr}}$ を持っているものとする。また、共有しようとする平文データとしてのファイルデータを m と表記する。サーバ装置 S_v は、グループ管理者 M 宛の暗号文 $E(p_{k_{Gr}}, m)$ をユーザ A (又はユーザ B 、又はユーザ C) 宛の暗号文 $E(p_{k_A}, m)$ (又は $E(p_{k_B}, m)$ 、又は $E(p_{k_C}, m)$) に再暗号化する再暗号化鍵 $r_{k_{Gr \rightarrow A}}$ (又は $r_{k_{Gr \rightarrow B}}$ 、又は $r_{k_{Gr \rightarrow C}}$) を持っているものとする。各ユーザ i は秘密鍵 s_{k_i} を持っているものとする。つまり、ユーザ A は秘密鍵 s_{k_A} を、ユーザ B は s_{k_B} を、ユーザ C は s_{k_C} をそれぞれ持っている。

[0038] 次に、ユーザ C は、公開鍵記憶部 11 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 $E(p_{k_{Gr}}, m)$ をサーバ装置 S_v へアップロードする。サーバ装置 S_v は、暗号文記憶部 12 においてこの暗号文を保管する。

[0039] 今、ユーザ A がファイルデータ m を共有したいとする。ユーザ A は、サーバ装置 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。サーバ装置 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 13 に記憶されているユーザ A 宛の再暗号化鍵 $r_{k_{Gr \rightarrow A}}$ に基づいて、暗号文 $E(p_{k_{Gr}}, m)$ をユーザ A 宛の再暗号文 $E(p_{k_A}, m)$ に再暗号化し、得られた再暗号文 $E(p_{k_A}, m)$ をユーザ A に送信する。ここで、再暗号文とは、暗号文を復号せずに再暗号化してなる暗号文である。

- [0040] ユーザAは、サーバ装置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。
- [0041] 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。
- [0042] 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M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M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。
- [0043] 本ファイル共有システムにおいて、サーバ装置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、サーバ装置S_vはこの暗号文を復号できない。これは、不正なサーバ装置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、サーバ装置S_vを厳重に管理しなくても良く、サーバ装置S_vの管理コストの低減に繋がる。
- [0044] ユーザBがファイル共有を行う際も上記と同様である。
- [0045] 図3は、ファイル共有システムに適用されるサーバ装置、ユーザ装置及びグループ管理者装置の構成を説明するための模式図である。なお、以下の構成の説明は、(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、(6) 再暗号化鍵更新処理のうち、(6) 再暗号化鍵の更新処理に関する内容を主に述べている。他の処理については、非特許文献1に開示されている。
- [0046] サーバ装置S_vは、グループ管理者の公開鍵（以下、管理者公開鍵ともいう）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、ユーザ装置の秘密鍵（以下、ユーザ秘密鍵ともいう）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記憶するものである。
- [0047] 具体的には、サーバ装置S_vは、公開鍵記憶部11、暗号文記憶部12、

再暗号化鍵記憶部 13、送受信部 14、再暗号化部 15、再暗号化鍵情報生成部 16 及び更新済み再暗号化鍵生成部 17 を備えている。

[0048] 公開鍵記憶部 11 は、各部 14～17 から読出／書込可能な記憶部であり、各ユーザの公開鍵やグループ管理者の公開鍵が記憶されている。

[0049] 暗号文記憶部 12 においては、各部 14～17 から読出／書込可能な記憶部であり、ユーザからアップロードされた暗号文が記憶されている。

[0050] 再暗号化鍵記憶部 13 は、各部 14～17 から読出／書込可能な記憶部であり、グループ管理者の公開鍵 g^x に対応する秘密鍵 x （以下、管理者秘密鍵ともいう）と、ユーザの秘密鍵 pw に対応する公開鍵 D （以下、ユーザ公開鍵ともいう）とに基づいて生成された再暗号化鍵 R （ $= D^{1/x} = g^{pw/x}$ ）を記憶するものである（ $\wedge$ はべき乗を表す記号）。また、再暗号化鍵記憶部 13 においては、更新前の再暗号化鍵 R を更新後の再暗号化鍵 W に置換可能（上書き可能）となっている。

[0051] 送受信部 14 は、サーバ装置 S_v と通信網との間の通信インタフェースであり、例えば、再暗号化鍵情報生成部 16 により計算（生成）された再暗号化鍵情報 Y （ $= R^h$ ）をユーザ装置（例、 B ）に送信し、ユーザ装置から更新前のユーザ秘密鍵 pw 及び更新後のユーザ秘密鍵 d に基づいて当該再暗号化鍵情報 Y から計算された再暗号化鍵更新情報 Z （ $= Y^{d/pw} = g^{d \cdot h/x}$ ）を受信する送受信機能をもっている。なお、説明を簡潔にするため、以下では送受信部 14 を介して送受信する旨の記載を適宜、省略する。

[0052] 再暗号化部 15 は、再暗号化鍵記憶部 13 において記憶されている再暗号化鍵を用いて暗号文を再暗号化する。再暗号化部 15 における具体的な処理については後述する。

[0053] 再暗号化鍵情報生成部 16 は、ユーザ装置 B から再暗号化鍵 R を更新する旨の通知を受けると、乱数 h を生成し、再暗号化鍵記憶部 13 に記憶された再暗号化鍵 R 及び当該生成した乱数 h に基づいて再暗号化鍵情報 Y （ $= R^h$ ）を計算する第 1 計算機能をもっている。

[0054] 更新済み再暗号化鍵生成部 17 は、送受信部 23 により受信された再暗号

化鍵更新情報 $Z (= Y ^ \{d/pw\} = g ^ \{d \cdot h/x\})$ 、及び再暗号化鍵情報生成部 16 により生成された乱数 h に基づいて更新後の再暗号化鍵 $W (= Z ^ \{1/h\} = g ^ \{d/x\})$ を計算すると共に、再暗号化鍵記憶部 12 内の再暗号化鍵 R を更新後の再暗号化鍵 W に置換する第 2 計算機能をもっている。

[0055] なお、再暗号化鍵 R は、サーバ装置 S_v により、乱数 h に基づいて再暗号化鍵情報 $Y (= R ^ h)$ が計算される情報でもある。

[0056] 再暗号化鍵情報 Y は、ユーザ装置 B により、更新前のユーザ秘密鍵 pw 及び更新後のユーザ秘密鍵 d に基づいて再暗号化鍵更新情報 $Z (= Y ^ \{d/pw\} = g ^ \{d \cdot h/x\})$ が計算される情報でもある。

[0057] 再暗号化鍵更新情報 Z は、サーバ装置 S_v により、乱数 h に基づいて更新後の再暗号化鍵 $W (= Z ^ \{1/h\} = g ^ \{d/x\})$ が計算される情報でもある。

[0058] 更新後の再暗号化鍵 W は、サーバ装置 S_v により更新前の再暗号化鍵 R から置換されて記憶される。

[0059] 一方、ユーザ装置 $A, B, C, \dots$ は、互いに同一のハードウェア構成であるため、ここではユーザ装置 B を例に挙げて説明する。

[0060] ユーザ装置 B は、秘密鍵記憶部 21、ファイルデータ記憶部 22、送受信部 23、鍵生成部 24、暗号化部 25、復号部 26 及び再暗号化鍵更新情報生成部 27 を備えている。

[0061] 秘密鍵記憶部 21 は、各部 23 ~ 27 から読出／書込可能な記憶部であり、更新前のユーザ公開鍵 $D = g ^ \{pw\}$ に対応する更新前のユーザ秘密鍵 pw と、更新後のユーザ公開鍵 $g ^ d$ に対応する更新後のユーザ秘密鍵 d とを記憶する。

[0062] ファイルデータ記憶部 22 は、各部 23 ~ 27 から読出／書込可能な記憶部であり、ファイルデータを記憶する。

[0063] 送受信部 23 は、ユーザ装置 B と通信網との通信インタフェースであり、例えば、再暗号化鍵 $R (= D ^ \{1/x\} = g ^ \{pw/x\})$ を更新する旨の通知をサーバ装置 S_v に送信し、サーバ装置 S_v から再暗号化鍵 R 及び乱数 h に基づいて計算された再暗号化鍵情報 $Y (= R ^ h)$ を受信する機能と、再暗号化鍵更

新情報生成部 27 により計算された再暗号化鍵更新情報 $Z (= Y ^ \{d/pw\} = g ^ \{d \cdot h/x\})$ をサーバ装置 S_v に送信する機能とを持っている。なお、説明を簡潔にするため、以下では送受信部 23 を介して送受信する旨の記載を適宜、省略する。

[0064] 鍵生成部 24 は、公開鍵・秘密鍵の組を生成する。また、鍵生成部 24 は、鍵生成に必要な各パラメータを保持している。鍵生成に必要な各パラメータについては後述する。

[0065] 暗号化部 25 は、サーバ装置 S_v から送受信部 23 を介して通知される（又は以前に取得した公開鍵で、ユーザ装置 B が記憶している）グループ管理者の公開鍵を用いて、ファイルデータ記憶部 22 に記憶されているファイルデータを暗号化する。

[0066] 復号部 26 は、秘密鍵記憶部 21 において記憶されているユーザの秘密鍵を用いて、再暗号文（又は暗号文）を復号する。

[0067] 再暗号化鍵更新情報生成部 27 は、送受信部 23 により受信した再暗号化鍵情報 $Y (= R ^ h)$ と、更新前のユーザ秘密鍵 pw 及び更新後のユーザ秘密鍵 d とに基づいて当該再暗号化鍵情報 Y から再暗号化鍵更新情報 $Z (= Y ^ \{d/pw\} = g ^ \{d \cdot h/x\})$ を計算する機能をもっている。

[0068] 他方、グループ管理者装置 M は、秘密鍵記憶部 31、送受信部 32、鍵生成部 33 及び再暗号化鍵生成部 34 を備えている。

[0069] 秘密鍵記憶部 31 は、各部 32～34 から読出／書込可能な記憶部であり、鍵生成部 33 において生成されたグループ管理者の管理者秘密鍵 x を記憶する。

[0070] 送受信部 32 は、グループ管理者装置 M と通信網との間の通信インタフェースであり、例えば、鍵生成部 33 において生成されたグループ管理者の公開鍵 $g ^ x$ をサーバ装置 S_v に送信する機能と、サーバ装置 S_v からユーザ装置 B のユーザ公開鍵 $D (= g ^ \{pw\})$ を受信する機能と、再暗号化鍵生成部 34 により生成された再暗号化鍵 R をサーバ装置 S_v に送信する機能とをもっている。

[0071] 鍵生成部33は、公開鍵・秘密鍵の組を生成する。また、鍵生成部33は、鍵生成に必要な各パラメータを保持している。

[0072] 再暗号化鍵生成部34は、送受信部32により受信したユーザ公開鍵 $D (= g^{\{pw\}})$ と、秘密鍵記憶部31内の管理者秘密鍵 x とに基づいて、再暗号化鍵 $R (= D^{\{1/x\}} = g^{\{pw/x\}})$ を生成（発行）する機能をもっている。本実施形態の一側面は、グループ管理者が不在の場合でも、つまり、グループ管理者の秘密鍵 x を用いずに、サーバ装置 S_v が更新前の再暗号化鍵 R を更新後の再暗号化鍵 W に更新し得る。

[0073] 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説明する。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、（６）再暗号化鍵更新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良い。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良い。また、再暗号化処理が実行されずに、暗号文が復号されても良い。また、（１）～（５）の処理は非特許文献1に開示されており、（６）の処理が本実施形態による再暗号化鍵の更新方法である。すなわち、再暗号化鍵の更新処理（６）以外の処理（１）～（５）については、非特許文献1を補足的に参照して理解を深めることができる。

[0074] （１．鍵セットアップ処理）始めに、鍵生成部33は、公開パラメータ（ $p, \lambda, G, G_T, g, u, v, \text{Sig}$ ）を生成する、又は外部から入手する（ $ST1$ ）。ここで、 λ はセキュリティパラメータである。 p は $p > 2\lambda$ を満たす素数である。 G, G_T は素数位数 $p > 2\lambda$ を満たす双線型写像群(bilinear map groups) (G, G_T)である。 g, u, v は、 G の生成元である（ $g, u, v \in G$ ）。 Sig は強偽造不可能性を満たす使い捨て署名（one-time signature）方式

[数1]

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

[0075] 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).に詳しい。

[0076] 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。

[0077] 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。

[0078] 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。

[0079] 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。

[0080] 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)。

[0081]
$$e(g_1 g_2, g) = e(g, g_1 g_2) = e(g, g^\alpha \cdot g^\beta) = e(g, g^{\alpha+\beta}) = e(g, g)^{\alpha+\beta} = e(g, g)^\alpha \cdot e(g, g)^\beta$$

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。

[0082] また、本明細書では、 G, G_T をともに乗法群と想定した記法を採用してい

るが、これに限らず、 G 、 G_T それぞれについて、加法群と想定した記法で表すことも可能である。つまり、例えば、 G を加法群、 G_T を乗法群として表現しても良い。また、双線型写像として、双線型写像群 G_1 、 G_2 、 G_T (G_1 と G_2 は異なる群である) について、 $e : G_1 \times G_2 \rightarrow G_T$ となる写像を用いても良い。これらは他の実施例においても同様である。

[0083] 鍵生成部33には、上記公開パラメータ (p , λ , G , G_T , g , u , v , Sig) が記憶されている。

[0084] 次に、鍵生成部33は、ユーザの識別情報を i としたとき、ユーザ i の秘密鍵 $x_i \in Z_p^*$ を生成し、この秘密鍵 x_i を用いてユーザ i の公開鍵

[数2]

$$X_i = g^{x_i}$$

[0085] 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。

[0086] ユーザ i の秘密鍵 x_i はユーザ i の秘密鍵記憶部21に記憶される。ユーザ i の公開鍵 X_i はサーバ装置 S_v の公開鍵記憶部11に記憶される。グループ管理者の秘密鍵・公開鍵についても同様に、グループ管理者の鍵生成部33において生成される。

[0087] (2. 暗号化处理) 暗号化部25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3]

$$\begin{aligned} & \hat{G} \text{ に基づいて、使い捨て署名における署名鍵 } ssk \text{ と検証鍵 } svk \text{ の鍵ペア} \\ & (ssk, svk) \leftarrow \hat{G}(\lambda) \end{aligned}$$

[0088] を生成し、第1暗号化データ C_1 に検証鍵 svk をセットする ($C_1 = svk$)。

[0089] 暗号化部25は、第1乱数 $r \in Z_p^*$ を生成する。暗号化部25は、この第1乱数 r に基づき、平文データとしてのメッセージ $m \in G_T$ に対して、以下の第

2、第3及び第4暗号化データ C_2 , C_3 , C_4 を生成する。

[数4]

$$\begin{aligned} C_2 &= X_i^r \\ C_3 &= e(g, g)^r \cdot m \\ C_4 &= (u^{svk} \cdot v)^r \end{aligned}$$

[0090] 具体的には、ユーザ i の公開鍵 X_i と、第1乱数 r とに基づいて、第2暗号化データ C_2 を生成する。また、公開パラメータにおける生成元 g と、第1乱数 r と、メッセージ m とに基づき、ペアリング関数によって第3暗号化データ C_3 を生成する。さらに、公開パラメータにおける生成元 u , v と、上記において生成した検証鍵 svk と、第1乱数 r とに基づいて、第4暗号化データ C_4 を生成する。

[0091] 暗号化部25は、第3及び第4暗号化データ C_3 , C_4 に対し、公開パラメータにおける署名生成機能

[数5]

$\hat{S}$ と、上記において生成した署名鍵 ssk による使い捨て署名 σ を次式に示すように生成する。

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

[0092] 上記の暗号化処理により得られる暗号文は、これら第1乃至第4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 $C_i = (C_1, C_2, C_3, C_4, \sigma)$ である。

[0093] (3. 再暗号化鍵生成処理) 再暗号化鍵生成部34は、秘密鍵記憶部31に記憶されている(本実施形態ではグループ管理者の)秘密鍵 x_i と、ユーザ j の公開鍵 X_j から、再暗号化鍵 R_{ij} を次式に示すように生成する。

[数6]

$$R_{ij} = X_j^{1/x_i} = g^{x_j/x_i}$$

[0094] 再暗号化鍵 R_{ij} は、ユーザ i 宛の暗号文を、ユーザ j 宛の再暗号文に再暗号化する際に用いられる。

[0095] (4. 再暗号化处理) ユーザ i 宛の暗号文を、ユーザ j 宛の再暗号文に再暗号化する処理を説明する。再暗号化部 15 は、公開パラメータと次の検証式を用い、暗号化处理において得られた暗号文 C_i を検証する。ここで、2つの検証式が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。

[数7]

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

$$\hat{v}(C_1, \sigma, (C_3, C_4)) \stackrel{?}{=} 1$$

[0096] 検証が成功した場合、再暗号化部 15 は、第2乱数 $t \in \mathbb{Z}_p^*$ を生成し、暗号化处理において得られた暗号文 C_i と、再暗号化鍵生成処理において得られた再暗号化鍵 R_{ij} とを用いて、次式に示すように、第1、第2及び第3再暗号化データ C_2' , C_2'' , C_2''' を生成する。

[数8]

$$C_2' = X_i^t$$

$$C_2'' = R_{ij}^{1/t} = g^{\left(\frac{x_j}{x_i} \right)^{t-1}}$$

$$C_2''' = C_2^t = X_i^{r \cdot t}$$

[0097] 具体的には、ユーザ i の公開鍵 X_i と、第2乱数 t とに基づいて、第1再暗号化データ C_2' を生成する。また、再暗号化鍵生成処理において得られた再暗号化鍵 R_{ij} 及び第2乱数 t に基づいて、第2再暗号化データ C_2'' を生成する。さらに、第2暗号化データ C_2 及び第2乱数 t に基づいて、第3再暗号化データ C_2''' を生成する。

[0098] 検証が失敗した場合は処理を終了する。

[0099] 上記の再暗号化处理により得られる再暗号文は、これら第1乃至第3再暗

号化データ $C_2' \sim C_2''''$ を、暗号文データ C_i 内の第2暗号化データ C_2 と置換して得られる再暗号文 $C_j = (C_1, C_2', C_2'', C_2''', C_2''', C_3, C_4, \sigma)$ である。

[0100] (5. 復号処理) ユーザ j が再暗号文を復号する処理を説明する。復号部 26 は、公開パラメータ及びユーザ j の公開鍵 X_j と次の検証式を用い、再暗号文 C_j を検証する。ここで、3つの検証式が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。

[数9]

$$\begin{aligned} e(C_2', C_2'') &\stackrel{?}{=} e(X_j, g) \\ e(C_2'', u^{C_1} \cdot v) &\stackrel{?}{=} e(C_2', C_4) \\ \hat{v}(C_1, \sigma, (C_3, C_4)) &\stackrel{?}{=} 1 \end{aligned}$$

[0101] 検証が成功した場合、復号部 26 は、ユーザ j の秘密鍵 x_j に基づいて、次式に示すように、再暗号化処理で得られた再暗号文 C_j を復号し、メッセージ m を得る。

[数10]

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

[0102] 検証が失敗した場合は処理を終了する。

[0103] 次に、本実施形態に係る (6) 再暗号化鍵の更新処理を説明する。図4は、再暗号化鍵の更新処理の概要を示す模式図である。なお、ファイル共有システムとしては図2において説明したものを想定する。ユーザ管理者 U は、グループ管理者を含めた全ユーザを管理するエンティティである。ユーザ管理者であるユーザ U は、ファイル共有システムに参加する各ユーザに、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 (ユーザ B に与える ID を ID と表記する) と初期パスワード (ユーザ B に与えるパスワード

を $p w$ と表記する) を発行する。パスワードは、ユーザ管理者 U により発行される仮の秘密鍵とみなすことができる。グループ管理者 M は、グループ管理者 M の秘密鍵 x と公開鍵 g^x とを生成する。以下、グループ管理者 M 宛の暗号文をユーザ B 宛の再暗号文に再暗号化するための再暗号化鍵を更新する際の処理を説明する。この更新処理には、ユーザ装置 B の秘密鍵 $p w$ とそれに対応する公開鍵の更新も伴う。

[0104] 図 5 及び図 6 は、再暗号化鍵の更新処理の動作を説明するためのフローチャートである。

[0105] ユーザ管理者装置 U は、ユーザ装置 B に対し、 $I D$ と初期パスワードを発行する (ステップ $S T 1$) 。

[0106] ユーザ管理者装置 U は、初期パスワード $p w$ を仮の秘密鍵と見立て、次式を用いて、これに対応する仮の公開鍵 D を生成し、サーバ装置 $S v$ へ送信する (ステップ $S T 2$) 。

[0107] $D = g^{pw}$

サーバ装置 $S v$ は、ユーザ管理者装置 U から送られてきた仮の公開鍵 D を公開鍵記憶部 11 に記憶する (ステップ $S T 3$) 。

[0108] 公開鍵と秘密鍵の組 (g^x, x) を持つグループ管理者装置 M は、サーバ装置 $S v$ に仮の公開鍵 D を要求し、サーバ装置 $S v$ はグループ管理者装置 M に仮の公開鍵 D を送信する (ステップ $S T 4$) 。グループ管理者装置 M は、再暗号化鍵生成部 34 において、次式を用いて、グループ管理者装置 M 宛の暗号文をユーザ装置 B 宛の再暗号文に再暗号化するための再暗号化鍵 R を生成し、サーバ装置 $S v$ へ送信する (ステップ $S T 5$) 。

[0109] $R = D^{1/x} = g^{pw/x}$

サーバ装置 $S v$ は、グループ管理者装置 M から受信した再暗号化鍵 R を再暗号化鍵記憶部 13 に記憶する (ステップ $S T 6$) 。

[0110] ユーザ装置 B は、ユーザ B の操作により、ステップ $S T 1$ で発行された $I D$ と初期パスワードを用いてファイル共有システムにログインし、サーバ装置 $S v$ に対して、再暗号化鍵を更新する旨の通知を行う (ステップ $S T 7$)

。

[0111] サーバ装置 S_v は、再暗号化鍵記憶部 13 より該当する再暗号化鍵（上述の例ではグループ管理者装置 M 宛の暗号文をユーザ装置 B 宛の再暗号文に再暗号化するための再暗号化鍵 R）を取得し、再暗号化鍵情報生成部 16 において、乱数 h を生成し、次式を用いて再暗号化鍵情報 Y を計算し、ユーザ装置 B に再暗号化鍵情報 Y を送信する（ステップ S T 8）。

$$[0112] \quad Y = R^h = g^{pw \cdot h/x}$$

ユーザ装置 B は、鍵生成部 24 において、新しい公開鍵と秘密鍵の組（（ g^d, d ）と表記する）を生成する（ステップ S T 9）。ユーザ装置 B は、秘密鍵記憶部 21 において秘密鍵 d を記憶する（ステップ S T 10）。ユーザ装置 B は、再暗号化鍵更新情報生成部 27 において次式を用いて再暗号化鍵更新情報 Z を計算し、サーバ装置 S_v に再暗号化鍵更新情報 Z と新しい公開鍵 g^d を送信する（ステップ S T 11）。

$$[0113] \quad Z = Y^{d/pw} = g^{d \cdot h/x}$$

サーバ装置 S_v は、公開鍵記憶部 11 において古い公開鍵 D を新しい公開鍵 g^d に置き換える（ステップ S T 12）。また、サーバ装置 S_v は、更新済み再暗号化鍵生成部 17 において、次式を用いて新しい再暗号化鍵 W を計算し、再暗号化鍵記憶部 13 において古い再暗号化鍵 R を新しい再暗号化鍵 W に置き換える（ステップ S T 13）。

$$[0114] \quad W = Z^{1/h} = g^{d/x}$$

上述の例では、グループ管理者が初めてファイル共有システムに参加する際の処理についての説明を省略したが、図 2 において説明したファイル共有システムでは、グループ管理者は、自身の公開鍵 pk_{Gr} をサーバ装置 S_v へ送信するだけで良いため、以下の処理を行えば良い。ユーザ管理者 U は、グループ管理者 M に対して、ID と初期パスワードを発行する。グループ管理者は、与えられた ID と初期パスワードを用いてファイル共有システムにログインする。グループ管理者は、鍵生成部 33 において、公開鍵 pk_{Gr} と秘密鍵 sk_{Gr} の組（ g^x, x ）を生成し（又は事前に生成しておき）、秘密鍵記憶部 3

1において秘密鍵 x ($= sk_{Gr}$)を記憶し、公開鍵 g^x ($= pk_{Gr}$)をサーバ装置 S_v へ送信する。サーバ装置 S_v は、公開鍵記憶部11において送られてきた公開鍵 g^x を記憶する。このようにしておけば、図2において、ユーザ C が、暗号文を生成する際に用いるグループ管理者の公開鍵 g^x をサーバ装置 S_v から取得することが可能となる。

[0115] なお、一度再暗号化鍵を更新した以降に、再び再暗号化鍵を更新する場合は、ステップ $ST7$ から処理を始めれば良い。この場合、初期のユーザ秘密鍵 pw を更新前のユーザ秘密鍵 d と読み替えれば良い。また、図5及び図6の各ステップは必ずしもこの順序で行わなくても良い。例えば、ステップ $ST8$ の処理の前にステップ $ST9$ 、ステップ $ST10$ の処理を行っても良いし、ステップ $ST8$ の処理とステップ $ST9$ 、ステップ $ST10$ の処理を同時に行っても良い。また、ステップ $ST12$ の処理とステップ $ST13$ の処理の順番を入れ替えて行っても良い。

[0116] このように再暗号化鍵の更新処理を行えば、再暗号化鍵の更新にグループ管理者の秘密鍵 x が不要になり、図5及び図6のステップ $ST6$ 以降グループ管理者の登場が不要となるため、グループ管理者が不在の場合でも再暗号化鍵を生成可能となる。また、サーバ装置 S_v にはグループ管理者の秘密鍵 x を知らせない構成のため、サーバ装置 S_v に対する（ファイルデータの）秘匿性も保たれる。また、ユーザに再暗号化鍵（上述の例では W ）を知らせない構成のため、再暗号化鍵の漏洩のリスクを抑えることができる。また、ユーザは、新しいユーザ秘密鍵（上述の例では d ）を他人に知らせる必要がないため、秘密鍵の漏洩のリスクを抑えることができる。また、（上述した再暗号化鍵の更新処理を行わず）グループ管理者の機能を有するプログラムを常時オンラインの PC に実装して自動応答させることで、グループ管理者 M が不在の場合でも再暗号化鍵を生成することが考えられる。しかしながら、この場合、当該グループ管理者の PC が常にオンラインであるため、外部からの攻撃を受ける恐れがあり、攻撃によってグループ管理者の秘密鍵 x を盗まれてしまうリスクが伴う。これに対し、上述した再暗号化鍵の更新処理

を行えば、このようなりスクを負うことなく安全に再暗号化鍵を生成することが可能となる。

[0117] 上述したように本実施形態によれば、サーバ装置S_vが、ユーザ装置Bから再暗号化鍵Rを更新する旨の通知を受けると、乱数hを生成し、再暗号化鍵記憶部13に記憶された再暗号化鍵R及び当該生成した乱数hに基づいて再暗号化鍵情報Y ($= R^h$) を計算し、この暗号化鍵情報Yをユーザ装置Bに送信し、ユーザ装置Bから更新前のユーザ秘密鍵pw及び更新後のユーザ秘密鍵dに基づいて当該再暗号化鍵情報Yから計算された再暗号化鍵更新情報Z ($= Y^{d/pw} = g^{d \cdot h/x}$) を受信し、この再暗号化鍵更新情報Z及び前述した乱数hに基づいて更新後の再暗号化鍵W ($= Z^{1/h} = g^{d/x}$) を計算すると共に、再暗号化鍵記憶部12内の再暗号化鍵Rを更新後の再暗号化鍵Wに置換する構成により、ユーザBのユーザ秘密鍵dをグループ管理者Mに知らせない場合、かつグループ管理者が不在の場合でも、再暗号化鍵を更新することができる。

[0118] [変形例1]

上述した実施形態では、サーバ装置S_vが乱数hを用い、再暗号化鍵Rのh乗の計算により再暗号化鍵情報Yを計算し、Zの1/h乗の計算により、更新後の再暗号化鍵Wを計算した。これに限らず、サーバ装置S_vが乱数hを用い、以下の各式に示すように、Xの1/h乗の計算により再暗号化鍵情報Y'を計算し、Z'のr乗の計算により、更新後の再暗号化鍵Wを計算してもよい。

$$[0119] \quad Y' = R^{1/h} = g^{pw/x \cdot h}$$

$$Z' = Y'^{d/pw} = g^{d/x \cdot h}$$

$$W = Z'^{1/h} = g^{d/x}$$

このような変形例1としても、本実施形態を同様に実施して同様の効果を得ることができる。

[0120] [変形例2]

上述した実施形態及び変形例では、再暗号化鍵Rをユーザに知られないよ

うにするために、サーバ装置 S v が乱数 h を用いて再暗号化鍵情報 Y を計算し、再暗号化鍵情報 Y をユーザへ送信する構成とした。これに限らず、再暗号化鍵 R をユーザに知られても良い場合は、サーバ装置 S v は、乱数 h の計算をせず、上述した実施形態又は変形例における再暗号化鍵情報 Y 又は Y' を、以下に示す Y'' に置き換えても良い。

[0121] $Y'' = R$

ここで、右辺の R は、上述した実施形態における再暗号化鍵 R を意味している。この場合、サーバ装置 S v は、上述した実施形態における再暗号化鍵 W を計算する必要はなく、ユーザから受信した再暗号化鍵更新情報 Z を新しい再暗号化鍵 W とすれば良い。

[0122] このように乱数 h を用いない場合、サーバ装置 S v においては、乱数 h を用いる再暗号化鍵情報生成部 1 6 及び更新済み再暗号化鍵生成部 1 7 が省略される。また、送受信部 1 4 は、例えば、ユーザ装置 B から再暗号化鍵 R を更新する旨の通知を受けると、再暗号化鍵 $R (= g^{\{pw/x\}})$ をユーザ装置 B に送信し、更新前のユーザ秘密鍵 pw 及び更新後のユーザ秘密鍵 d に基づいて当該再暗号化鍵 R から計算された更新後の再暗号化鍵 $W (= g^{\{d/x\}})$ をユーザ装置 B から受信する送受信機能と、再暗号化鍵記憶部 1 3 内の再暗号化鍵 R を更新後の再暗号化鍵 W に置換する置換機能とをもつものとすればよい。各記憶部 1 1 ~ 1 3 は、実施形態と同様のものでよい。

[0123] このような変形例 2 によれば、本実施形態と同様の効果に加え、再暗号化鍵 R をユーザに知られてもよい場合には乱数 h を用いた計算を省略することができる。

[0124] (第 2 の実施形態)

非特許文献 2 の 3 章に記載の "A Second Attempt" の方式では、再暗号化鍵の形式が第 1 の実施形態と同様の数式から成り立っているため、第 1 の実施形態の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、復号処理をそれぞれ非特許文献 2 の "A Second Attempt" の処理に置き換えることにより、非特許文献 2 の "A Second Attempt" の方式において

も第1の実施形態に対するのと同様の技術的效果を得ることができる。

[0125] (第3の実施形態)

非特許文献2の3章に記載の”A Third Attempt”の方式では、再暗号化鍵の形式が第1の実施形態が $g^{\{pw/x\}}$ であるのに対して、 $g^{\{pw \cdot x\}}$ の形をしている。そのため、図7に示すように、 $R=D^x$ とし、第1の実施形態の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、復号処理をそれぞれ非特許文献2の”A Third Attempt”の処理に置き換えることにより、非特許文献2の”A Third Attempt”の方式においても第1の実施形態に対するのと同様の技術的效果を得ることができる。

[0126] (第4の実施形態)

非特許文献2の3.2節に記載の”Temporary Unidirectional Proxy Re-encryption”の方式では、再暗号化鍵の形式が第1の実施形態が $g^{\{pw/x\}}$ であるのに対して、 $g^{\{pw \cdot xr/x0\}}$ の形をしている。そのため、図8に示すように、 $R=D^{\{xr/x0\}}$ とし、第1の実施形態の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、復号処理をそれぞれ非特許文献2の”Temporary Unidirectional Proxy Re-encryption”の処理に置き換えることにより、非特許文献2の”Temporary Unidirectional Proxy Re-encryption”の方式においても第1の実施形態に対するのと同様の技術的效果を得ることができる。

[0127] 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。

[0128] 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。

[0129] 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。

[0130] 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。

[0131] 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。

[0132] 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。

[0133] 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。

[0134] 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]

管理者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、ユーザ装置（A， B， C， …）のユーザ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記憶するサーバ装置（S v）であって、

前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を記憶する記憶手段（1 3）と、

前記ユーザ装置から前記再暗号化鍵を更新する旨の通知を受けると、前記再暗号化鍵を前記ユーザ装置に送信し、更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて当該再暗号化鍵から計算された更新後の再暗号化鍵を前記ユーザ装置から受信する送受信手段（1 4）と、

前記記憶手段内の再暗号化鍵を前記更新後の再暗号化鍵に置換する置換手段（1 7）と、

を備えたことを特徴とするサーバ装置。

[請求項2]

管理者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、ユーザ装置（A， B， C， …）のユーザ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記憶するサーバ装置（S v）であって、

前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を記憶する記憶手段（1 3）と、

前記ユーザ装置から前記再暗号化鍵を更新する旨の通知を受けると、乱数を生成し、前記記憶された再暗号化鍵及び前記生成した乱数に基づいて再暗号化鍵情報を計算する第1 計算手段（1 6）と、

前記再暗号化鍵情報を前記ユーザ装置に送信し、前記ユーザ装置から更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて当

該再暗号化鍵情報から計算された再暗号化鍵更新情報を受信する送受信手段（１４）と、

前記再暗号化鍵更新情報及び前記乱数に基づいて前記更新後の再暗号化鍵を計算すると共に、前記記憶手段内の再暗号化鍵を前記更新後の再暗号化鍵に置換する第２計算手段（１７）と、

を備えたことを特徴とするサーバ装置。

[請求項3]

管理者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、ユーザ装置（Ａ，Ｂ，Ｃ，…）のユーザ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記憶するサーバ装置（Ｓｖ）のプロセッサに実行され、非一時的なコンピュータ読取り可能な記憶媒体（Ｍ１）に記憶されたプログラムであって、

前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を前記サーバ装置の記憶手段（１３）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、

前記ユーザ装置から前記再暗号化鍵を更新する旨の通知を受けると、前記再暗号化鍵を前記ユーザ装置に送信し、更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて当該再暗号化鍵から計算された更新後の再暗号化鍵を前記ユーザ装置から受信する処理を前記プロセッサに実行させる第２プログラムコード（１４）、

前記記憶手段内の再暗号化鍵を前記更新後の再暗号化鍵に置換する処理を前記プロセッサに実行させる第３プログラムコード（１７）、
を備えたプログラム。

[請求項4]

管理者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、ユーザ装置（Ａ，Ｂ，Ｃ，…）のユーザ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記憶するサーバ装置（Ｓｖ）のプロセッサに実行され、非一時的なコン

コンピュータ読取り可能な記憶媒体（M1）に記憶されたプログラムであって、

前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を前記サーバ装置の記憶手段（13）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、

前記ユーザ装置から前記再暗号化鍵を更新する旨の通知を受けると、乱数を生成し、前記記憶された再暗号化鍵及び前記生成した乱数に基づいて再暗号化鍵情報を計算する処理を前記プロセッサに実行させる第2プログラムコード（16）、

前記再暗号化鍵情報を前記ユーザ装置に送信し、前記ユーザ装置から更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて当該再暗号化鍵情報から計算された再暗号化鍵更新情報を受信する処理を前記プロセッサに実行させる第3プログラムコード（14）、

前記再暗号化鍵更新情報及び前記乱数に基づいて前記更新後の再暗号化鍵を計算すると共に、前記記憶手段内の再暗号化鍵を前記更新後の再暗号化鍵に置換する処理を前記プロセッサに実行させる第4プログラムコード（17）、

を備えたプログラム。

[請求項5]

管理者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、ユーザ装置（A，B，C，…）のユーザ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であって、前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を記憶するサーバ装置（Sv）に通信可能な前記ユーザ装置のプロセッサに実行され、非一時的なコンピュータ読取り可能な記憶媒体（M4）に記憶されたプログラムであって、

更新前のユーザ公開鍵に対応する更新前のユーザ秘密鍵と、更新後

のユーザ公開鍵に対応する更新後のユーザ秘密鍵とを前記ユーザ装置の記憶手段（２１）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、

前記再暗号化鍵を更新する旨の通知を前記サーバ装置に送信し、前記サーバ装置から前記再暗号化鍵及び乱数に基づいて計算された再暗号化鍵情報を受信する処理を前記プロセッサに実行させる第２プログラムコード（２３）、

前記受信した再暗号化鍵情報と、前記更新前のユーザ秘密鍵及び前記更新後のユーザ秘密鍵とに基づいて当該再暗号化鍵情報から再暗号化鍵更新情報を計算する処理を前記プロセッサに実行させる第３プログラムコード（２７）、

前記計算した再暗号化鍵更新情報を前記サーバ装置に送信する処理を前記プロセッサに実行させる第４プログラムコード（２３）、

を備えており、

前記再暗号化鍵更新情報は、前記サーバ装置により、前記乱数に基づいて更新後の再暗号化鍵が計算される情報であり、

前記更新後の再暗号化鍵は、前記サーバ装置により、更新前の再暗号化鍵から置換されて記憶されるプログラム。

[請求項6]

グループ管理者装置の管理者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、ユーザ装置（Ａ，Ｂ，Ｃ，…）のユーザ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であって、前記管理者公開鍵に対応する管理者秘密鍵と、前記ユーザ秘密鍵に対応するユーザ公開鍵とに基づいて生成された前記再暗号化鍵を記憶するサーバ装置（Ｓｖ）に通信可能な前記グループ管理者装置（Ｍ）のプロセッサに実行され、非一時的なコンピュータ読取り可能な記憶媒体（Ｍ３）に記憶されたプログラムであって、

前記管理者秘密鍵を前記グループ管理者装置の記憶手段（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、

前記サーバ装置から受けた前記ユーザ公開鍵と、前記管理者秘密鍵とに基づいて、前記再暗号化鍵を生成する処理を前記プロセッサに実行させる第2プログラムコード(34)、

前記生成した再暗号化鍵を前記サーバ装置に送信する処理を前記プロセッサに実行させる第3プログラムコード(32)、

を備えており、

前記再暗号化鍵は、前記サーバ装置により、乱数に基づいて再暗号化鍵情報が計算される情報であり、

前記再暗号化鍵情報は、前記ユーザ装置により、更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて再暗号化鍵更新情報が計算される情報であり、

前記再暗号化鍵更新情報は、前記サーバ装置により、前記乱数に基づいて更新後の再暗号化鍵が計算される情報であり、

前記更新後の再暗号化鍵は、前記サーバ装置により更新前の再暗号化鍵から置換されて記憶されるプログラム。