

明 細 書

発明の名称：

再暗号文検証プログラム、再暗号化装置及び再暗号化システム

技術分野

[0001] 本発明の実施形態は、再暗号文検証プログラム、再暗号化装置及び再暗号化システムに関する。

背景技術

[0002] 1998年にブレイズ (Blaze) らにより、公開鍵暗号系に関してプロキシ再暗号化 (Proxy Re-Encryption) と呼ばれる技術が提案されている。

[0003] この技術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。

[0004] (鍵生成) $\text{KeyGen}(1^k) \rightarrow (pk, sk)$

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

[0005] (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。

[0006] (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。

[0007] (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。

[0008] (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。

[0009] 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。

[0010] 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。

[0011] 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。

[0012] 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。

[0013] 具体的な方式の例としては、一方向性モデルでは非特許文献3, 4に記載の方式が、双方向性モデルでは非特許文献5に記載の方式が、IDベース暗号では非特許文献6, 7などに記載の方式がそれぞれ知られている。なお、実施形態では非特許文献8に記載の方式を参考にしている。

[0014] 図9はこのような再暗号化技術を説明するためのコンテンツ配信システムの一例を示す模式図である。このコンテンツ配信システムは、コンテンツプロバイダ1、配信システム2及びユーザ3という3者のエンティティからなる。なお、ユーザ3は、各々のユーザを区別する場合にはユーザA又はユーザBと呼ぶ。

[0015] 事前準備として、コンテンツプロバイダ1は、配信システム2の公開鍵 $p k_{Gr}$ を持っているものとする。配信システム2は、配信システム2宛の暗号文

コンテンツ $E(p k_{Gr}, M)$ を特定のユーザ A 又は B 宛の暗号文コンテンツ $E(p k_A, M)$ 又は $E(p k_B, M)$ に再暗号化する再暗号化鍵 $r k_{Gr \rightarrow A}$, $r k_{Gr \rightarrow B}$ を持っているものとする。各ユーザ 3 は自分宛の再暗号文コンテンツ $E(p k_A, M)$ 又は $E(p k_B, M)$ を復号する秘密鍵 $s k_A$ 又は $s k_B$ を持っているものとする。その他の各種の鍵やパラメータの説明は省略する。

[0016] 次に、コンテンツプロバイダ 1 は、コンテンツ M を配信システム 2 の公開鍵 $p k_{Gr}$ で暗号化し、得られた暗号文コンテンツ $E(p k_{Gr}, M)$ を配信システム 2 に配布する。

[0017] 配信システム 2 は、コンテンツプロバイダ 1 から暗号文コンテンツ $E(p k_{Gr}, M)$ を受ける。その後、配信システム 2 は、例えばユーザ A から受けたコンテンツ要求に対し、特定のユーザ A 宛の再暗号化鍵 $r k_{Gr \rightarrow A}$ に基づいて、暗号文コンテンツ $E(p k_{Gr}, M)$ をユーザ A 宛の再暗号文コンテンツ $E(p k_A, M)$ に再暗号化し、得られた再暗号文コンテンツ $E(p k_A, M)$ をユーザ A に配布する。

[0018] ユーザ A は、任意の配信システム 2 から受けた再暗号文コンテンツ $E(p k_A, M)$ を自身が保有する秘密鍵 $s k_A$ で復号し、得られたコンテンツ M を利用する。

[0019] 以上のようなコンテンツ配信システムは、コンテンツプロバイダ 1 による暗号化からユーザ A による復号までの間、コンテンツ M が一度も復号されないため、コンテンツ配信の過程における情報の漏洩を阻止することができる。

[0020] また、コンテンツプロバイダ 1 は、ユーザ 3 を特定せずに、配信システム 2 の公開鍵 $p k_{Gr}$ で暗号化することから、管理する鍵が配信システム 2 の公開鍵 $p k_{Gr}$ のみでよいので、鍵管理のコストを低減させることができる。

[0021] 配信システム 2 は、暗号文コンテンツ $E(p k_{Gr}, M)$ を復号せずにユーザ 3 宛に再暗号化することから、再暗号化に用いるサーバを厳重に管理しなくてもよいので、コストを低減させることができる。

[0022] ユーザ 3 は、単純に配信システム 2 にコンテンツ要求を出すだけで、これ

まで同様に任意のコンテンツMを利用することができる。

先行技術文献

特許文献

[0023] 特許文献1：特開 2 0 0 4 － 3 6 3 7 7 9 号公報

特許文献2：特許第 4 0 1 0 7 6 6 号公報

非特許文献

[0024] 非特許文献1：M. Blaze, M. Strauss. Atomic Proxy Cryptography. AT&T Labs Research TR98.5.1, 1997.

非特許文献2：M. Blaze, G. Bleumer, M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In Eurocrypt' 98, LNCS 1403, pp. 127-144, 1998.

非特許文献3：G. Ateniese, K. Fu, M. Green, S. Hohenberger. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. In NDSS' 05, 2005.

非特許文献4：B. Libert, D. Vergnaud. Tracing Malicious Proxies in Proxy Re-Encryption. In Pairing 2008, 2008.

非特許文献5：R. Canetti, S. Hohenberger. Chosen-Ciphertext Secure Proxy Re-Encryption. In ACM CCS' 07, 2005.

非特許文献6：M. Green, G. Ateniese. Identity-Based Proxy Re-encryption. In ACNS' 07, 2007.

非特許文献7：T. Matsuo. Proxy Re-encryption Systems for Identity-based Encryption. In Pairing 2007, 2007.

非特許文献8：Benoit Libert, Damien Vergnaud, " Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption" , Public Key Cryptography 2008 , pp.360-279

非特許文献9：G. Ateniese, S. Hohenberger, " Proxy re-signature: new definitions, algorithm, and applications" , ACM Conference on Computer and Communications Security 2005, pp.310-319

非特許文献10：A. Menezes, P. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, (1996),

発明の概要

発明が解決しようとする課題

[0025] しかしながら以上のような再暗号化技術は、通常は特に問題ないが、本発明者の検討によれば、次のような不都合がある。

[0026] 従来の暗号システムは、暗号化する人と復号する人という2者のエンティティからなるため、復号する人を特定できればよい。これに対し、再暗号化技術において復号する人は、誰から再暗号文データを受けるか分からない場合には、元々誰宛の暗号文データが再暗号化されたのかを検証できない不都合がある。

[0027] 例えば、再暗号化技術では、再暗号化鍵を生成する機能と再暗号化を行う機能とを分離できるので、これらの機能を別のエンティティに実装する場合がある。この場合、復号するユーザは、再暗号化を行ったエンティティから再暗号文コンテンツを受けたとしても、元々誰宛の暗号文コンテンツが再暗号化されたのかを検証する手段がない。

[0028] よって、ユーザ、または漏洩した原因を調査する第三者は、仮に、漏洩した暗号文コンテンツを再暗号化した状態で受けたとしても、この状態から元々誰宛の暗号文コンテンツだったのかを検証できないため、漏洩元を特定することが困難となる。

[0029] なお、上述した不都合の解消を図る技術の候補として、例えばプロキシ再署名 (Proxy Re-Signature) が知られている。但し、この技術は署名の付け替えを行う方式であるため、前述した再暗号化機能を実現する再暗号化システム (Proxy Re-encryption) と再署名システム (Proxy Re-Signature) とを組み合わせる必要がある。しかしながら、この組み合わせは、両者の機能を実現するための計算量やデータ長が大きくなることに加え、両者のシステムを連携させる好適な方法が知られていないことから、実現が困難である。

[0030] 不都合の解消を図る別の候補として、再暗号化システム(Proxy Re-Encryption)に既存の電子署名システムを組み合わせる技術が提案されている。しかしながら、この技術は、暗号化する人と再暗号化する人がどのデータにどのように電子署名を施せばよいのかが現状では知られていないため、実現が困難である。

[0031] すなわち、再暗号化技術は、前述した不都合が未だ解消されていない状況にある。

[0032] 本明細書に開示した実施形態は、再暗号文データを受けた復号装置が、元々誰宛の暗号文データが再暗号化されたのかを検証し得る再暗号文検証プログラム、再暗号化装置及び再暗号化システムを提供することを目的とする。

[0033] そのため、本明細書では、再暗号化鍵を生成する機能と再暗号化を行う機能とを別のエンティティにより行う場合について説明する。

課題を解決するための手段

[0034] 実施形態の再暗号化システムは、暗号化装置、再暗号化鍵生成装置、再暗号化装置及び復号装置を備えている。

[0035] 前記暗号化装置においては、第1記憶手段が前記再暗号化装置の公開鍵を記憶する。暗号化手段は、前記第1記憶手段から読み出した前記再暗号化装置の公開鍵を用いて前記平文データを暗号化処理することにより、暗号文データを得る。前記暗号化装置は、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。

[0036] 前記再暗号化鍵生成装置においては、第2記憶手段が、前記再暗号化装置の公開鍵に対応する秘密鍵と、前記復号装置の秘密鍵に対応する公開鍵とを記憶する。前記再暗号化鍵生成装置は、前記第2記憶手段から読み出した前記再暗号化装置の秘密鍵と前記復号装置の公開鍵とを用いて再暗号化鍵を生成する。前記再暗号化鍵生成装置は、前記生成された再暗号化鍵を前記再暗号化装置に送信する。

[0037] 前記再暗号化装置においては、第3記憶手段が、前記再暗号化鍵生成装置から受けた再暗号化鍵を記憶する。再暗号化手段は、前記暗号化装置から暗

号文データを受けると、前記第3記憶手段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処理することにより、再暗号文データを得る。前記再暗号化装置は、前記得られた再暗号文データを前記復号装置に送信する。

[0038] 前記復号装置は、第4記憶手段、復号手段、保持手段、判定手段及び出力手段を備えている。第4記憶手段は、前記再暗号化装置の公開鍵と前記復号装置の秘密鍵を記憶する。

[0039] 復号手段は、前記再暗号化装置から再暗号文データを受けると、前記第4記憶手段から読み出した当該復号装置の秘密鍵に基づいて、当該再暗号文データを復号処理することにより、前記平文データを得る。

[0040] 保持手段は、前記再暗号化システムに用いられる再暗号文データの一部と、当該再暗号文データを再暗号化処理する前の暗号文データの暗号化処理に用いられた公開鍵と、当該再暗号文データを復号可能な秘密鍵とが代入された場合に成立する検証式を予め保持する。

[0041] 判定手段は、前記保持手段から読み出した検証式に基づき、前記再暗号化装置から受けた再暗号文データの一部と、前記第4記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵と前記復号装置の秘密鍵とを当該検証式に代入して演算を実行することにより、この検証式が成立するか否かを判定する。

[0042] 出力手段は、この判定の結果、前記検証式が成立したとき、前記平文データの暗号化処理に用いられた公開鍵が前記再暗号化鍵生成装置の公開鍵であった旨を示す検証成功を出力する。

図面の簡単な説明

[0043] [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、第2の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8]図8は、第2の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9]図9は、一般的な再暗号化技術を説明するためのコンテンツ配信システムの一例を示す模式図である。

発明を実施するための形態

[0044] 以下、各実施形態について図面を用いて説明する。なお、以下の各装置は、それぞれハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、図1に示す如き、予めネットワーク又は非一時的なコンピュータ読取可能な記憶媒体（non-transitory computer-readable storage medium）M1～M5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、当該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。

[0045] （第1の実施形態）

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。この再暗号化システムは、鍵生成装置10、暗号化装置20、再暗号化鍵生成装置30、再暗号化装置40及び復号装置50を備えている。ここで、鍵生成装置10は、再暗号化システムの各種パラメータ及び各装置40、50の公開鍵・秘密鍵のペアを生成する。

- [0046] 暗号化装置 20 は、再暗号化鍵生成装置 30 の秘密鍵に対応する公開鍵を用いて平文データを暗号化処理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。
- [0047] 再暗号化鍵生成装置 30 は、再暗号化鍵生成装置 30 の秘密鍵と復号装置 50 の公開鍵とを用いて再暗号化鍵を生成し、その後その再暗号化鍵を再暗号化装置 40 に送信する。
- [0048] 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、再暗号化鍵生成装置 30 から送信された再暗号化鍵により再暗号化処理して得られた再暗号文データを復号装置 50 に送信する。
- [0049] 復号装置 50 は、再暗号化鍵生成装置 30 の公開鍵を用いて再暗号文データを検証処理すると共に、自装置 50 の公開鍵に対応する秘密鍵を用いて再暗号文データを復号処理して平文データを得る。なお、再暗号化鍵生成装置 30、再暗号化装置 40 及び復号装置 50 は、それぞれ複数台が設けられていてもよいが、ここでは一台ずつ設けられている場合を例に挙げて述べる。
- [0050] 続いて、各装置 10～50 の構成を具体的に説明する。
- [0051] 鍵生成装置 10 は、鍵生成パラメータ記憶部 11、一時データ記憶部 12、公開パラメータ生成部 13、公開鍵・秘密鍵生成部 14、通信部 15 及び制御部 16 を備えている。
- [0052] 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。
- [0053] 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。
- [0054] 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。
- [0055] 公開鍵・秘密鍵生成部 14 は、ユーザ宛の公開鍵・秘密鍵を生成する。
- [0056] 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 内の各 30、50 の公開鍵・秘密鍵のペアを当該各装置 30、50 に送信する機能と、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、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。

[0057] 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。

[0058] 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。

[0059] ここで、一時データ記憶部 21 は、鍵生成装置 10 から受けた再暗号化鍵生成装置 30 の公開鍵や、各生成部 23、24 の処理途中及び処理結果などの一時的なデータ（以下、一時データともいう）を記憶する記憶装置である。

[0060] 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 に公開された再暗号化鍵生成装置 30 の公開鍵を取得して一時データ記憶部 21 に書き込む機能や、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。

[0061] 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。

[0062] 暗号文生成部 24 は、一時データ記憶部 21 から読み出した再暗号化鍵生成装置 30 の公開鍵を用いて平文データを暗号化処理することにより、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。

[0063] 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。

[0064] 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 及び制御部 35 を備えている。

[0065] 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。

[0066] 一時データ記憶部 32 は、鍵生成装置 10 から受けた復号装置 50 の公開鍵や、再暗号化鍵生成部 34 の処理途中及び処理結果などの一時データを記憶する記憶装置である。

[0067] 通信部 33 は、他の装置 10, 20, 40, 50 と通信するための通信インタフェースであり、例えば制御部 35 に制御されて一時データ記憶部 32 内の再暗号化鍵を再暗号化装置 40 に送信する機能をもっている。

[0068] 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 の秘密鍵と、一時データ記憶部 32 から読み出した復号装置 50 の公開鍵とを用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。

[0069] 制御部 35 は、図 4 に示す動作を実行するように、各部 31 ~ 34 を制御する機能をもっている。

[0070] 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、検証プログラム記憶部 45、配信部 46 及び制御部 47 を備えている。

[0071] 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。

[0072] 一時データ記憶部 42 は、再暗号化処理部 44 の処理途中及び処理結果などの一時データを記憶する記憶装置である。

[0073] 通信部 43 は、他の装置 10 ~ 30, 50 と通信するための通信インタフェースであり、例えば、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 47 に制御されて一時データ記憶部 42 内の再暗号文データを復号装置 50 に送信する機能と、配信部 46 に制御されて検証プログラム記憶部 45 内の再暗号文検証プログラムを復号装置 50 に送信する機能とをもっている。

[0074] 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を用いて当該暗号文データを

復号せずに再暗号化処理することにより、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 4 2 に書き込む機能とをもっている。

[0075] 検証プログラム記憶部 4 5 は、再暗号文検証プログラムを記憶する記憶装置である。なお、再暗号化鍵記憶部 4 1 及び検証プログラム記憶部 4 5 は、同一の記憶装置における別々の記憶領域として実現してもよく、別々の記憶装置として実現してもよい。

[0076] 配信部 4 6 は、この再暗号文検証プログラムの配信要求を復号装置 5 0 から受けると、検証プログラム記憶部 4 5 内の再暗号文検証プログラムを通信部 4 3 から当該復号装置 5 0 に配信する機能をもっている。

[0077] なお、検証プログラム記憶部 4 5 は、再暗号化装置 4 0 にあり、そこから検証プログラム記憶部 4 5 内の再暗号文検証プログラムが配信部 4 6 を通じて配信されることになっているが、再暗号化装置 4 0 以外から配信されても良い。上記で説明したのはあくまでも実施形態の一例であり、再暗号化装置 4 0 以外から配信されることも考えられるからである。具体的には、鍵生成装置 1 0 から以下で説明する復号装置 5 0 への配信や、再暗号化鍵生成装置 3 0 から以下で説明する復号装置 5 0 への配信も考えられる。

[0078] 制御部 4 7 は、再暗号文検証プログラムを配信する動作（図示せず）と図 5 に示す動作を実行するように、各部 4 1 ～ 4 6 を制御する機能をもっている。

[0079] 復号装置 5 0 は、秘密鍵記憶部 5 1、一時データ記憶部 5 2、通信部 5 3、復号処理部 5 4、暗号文検証処理部 5 5 及び制御部 5 6 を備えている。

[0080] 秘密鍵記憶部 5 1 は、鍵生成装置 1 0 から受けた自装置 5 0 の秘密鍵を記憶する記憶装置である。

[0081] 一時データ記憶部 5 2 は、鍵生成装置 1 0 から受けた自装置 5 0 の公開鍵及び再暗号化鍵生成装置 3 0 の公開鍵や、復号処理部 5 4 及び暗号文検証処理部 5 5 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。

[0082] 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 から受けた自装置 50 の公開鍵及び再暗号化鍵生成装置 30 の公開鍵を一時データ記憶部 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。

[0083] 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。

[0084] 暗号文検証処理部 55 は、以下の各機能(f55-1)～(f55-3)をもっている。

[0085] (f55-1) 再暗号化システムに用いられる再暗号文データの一部と、当該再暗号文データを再暗号化処理する前の暗号文データの暗号化処理に用いられた公開鍵と、当該再暗号文データを復号可能な秘密鍵とが代入された場合に成立する検証式を予め保持する保持機能。なお、検証式を予め保持する保持機能は、検証式が予め記述されたプログラムコードを保持する保持機能と読み替えてもよい。

[0086] (f55-2) 保持機能から読み出した検証式に基づき、再暗号化装置から受けた再暗号文データの一部と、一時データ記憶部 52 から読み出した再暗号化鍵生成装置 30 の公開鍵と秘密鍵記憶部 51 内の復号装置 50 の秘密鍵とを当該検証式に代入して演算を実行することにより、この検証式が成立するかどうかを判定する判定機能。

[0087] (f55-3) この判定の結果、検証式が成立したとき、平文データの暗号化処理に用いられた公開鍵が再暗号化鍵生成装置 30 の公開鍵であった旨を示す検証成功を出力する機能。

[0088] 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。

[0089] 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。なお、復号装置 50 においては、予め再暗号文検証プログラムの配信要求を再暗号化装置 40 に送信しており、再暗号化装置 40 の配信部 46 から受信した再暗号文検証プログラムを実行中であるものとする。

[0090] 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。

[0091] また、以下の動作は、復号装置 50 内の暗号文検証処理部 55 の処理を除き、非特許文献 8 に記載の技術を例に用いている。すなわち、暗号文検証処理部 55 の処理以外の処理については、非特許文献 8 を補足的に参照して理解を深めることができる。

[0092] （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。

[0093] 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 $(p, \lambda, G, G_T, g, u, v, \text{Sig})$ を生成する (S T 1)。具体的には、公開パラメータ生成部 13 は、予め鍵パラメータ記憶部 11 に記憶したセキュリティパラメータ λ に基づいて、素数位数 $p > 2\lambda$ を満たす双線型写像群 (bilinear map groups) (G, G_T) 、生成元 $g, u, v \in G$ 、強偽造不可能性を満たす使い捨て署名 (one-time signature)

[数 1]

$\text{Sig}(\hat{G}, \hat{S}, \hat{V})$ を選択する。

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。

[0094] 使い捨て署名については非特許文献 10 に詳しい。また、 G 、 G_T は楕円曲線で定義される群集合であり、次式に示す如きペアリング関数に用いられる。

[0095] ペアリング関数： $e(g_1, g_2) = g_T$

但し、 $g_1, g_2 \in G$ 、 $g_T \in G_T$

このペアリング関数は、次式に示す如き性質がある。

[0096] $e(g^a, g) = e(g, g^a) = e(g, g)^a$

但し、 $g \in G$ 、 $a \in \mathbb{Z}_p$

続いて、公開パラメータ生成部 13 は、生成した公開パラメータを一時データ記憶部 12 に書き込む。鍵生成装置 10 は、一時データ記憶部 12 内の公開パラメータ ($p, \lambda, G, G_T, g, u, v, \text{Sig}$) を公開する (ST2)。

[0097] また、公開鍵・秘密鍵生成部 14 は、再暗号化鍵生成装置 30 の識別情報を i としたとき、再暗号化鍵生成装置 30 の秘密鍵 $x_i \in \mathbb{Z}_p^*$ を生成し、この秘密鍵 x_i を用いて再暗号化鍵生成装置 30 の公開鍵

[数2]

$$X_i = g^{x_i}$$

[0098] を生成する (ST7)。なお、 $\mathbb{Z}_p^*$ は $\mathbb{Z}_p$ かつ p と互いに素な整数の集合 ($(\mathbb{Z}/p\mathbb{Z})^*$) であり、素数 p に対する乗法群 $\mathbb{Z}_p^*$ と呼んでもよい。 $\mathbb{Z}_p$ は 0 以上 p 未満の整数の集合 ($(\mathbb{Z}/p\mathbb{Z})$) である。

[0099] 続いて、公開鍵・秘密鍵生成部 14 は、生成した公開鍵・秘密鍵のペアを一時データ記憶部 12 に書き込む。通信部 15 は、制御部 16 に制御されて一時データ記憶部 12 内の秘密鍵 x_i を再暗号化鍵生成装置 30 に送信する (ST8)。鍵生成装置 10 は、一時データ記憶部 12 内の再暗号化鍵生成装置 30 の公開鍵 X_i を公開する (ST9)。

[0100] また同様に、公開鍵・秘密鍵生成部 14 は、復号装置 50 の識別情報を j としたとき、復号装置 50 の秘密鍵 $x_j \in \mathbb{Z}_p^*$ を生成し、この秘密鍵 x_j を用い

て復号装置 50 の公開鍵

[数3]

$$X_j = g^{x_j}$$

[0101] を生成する (S T 1 0)。

[0102] 続いて、公開鍵・秘密鍵生成部 14 は、生成した公開鍵・秘密鍵のペアを一時データ記憶部 12 に書き込む。通信部 15 は、制御部 16 に制御されて一時データ記憶部 12 内の秘密鍵 x_j を復号装置 50 に送信する (S T 1 1)。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 X_j を公開する (S T 1 2)。また、所望により、暗号化装置 20 の秘密鍵 x_h 及び公開鍵 X_h についても各ステップ S T 1 0 ~ S T 1 2 と同様の処理を実行して暗号化装置 20 に秘密鍵 x_h を送信し、公開鍵 X_h を公開してもよい。

[0103] 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 S T 2, S T 9, S T 1 2 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。

[0104] (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 S T 2 1 ~ S T 2 4 に示すように実行される。

[0105] 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4]

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

[0106] を生成し (S T 2 1)、第 1 暗号化データ C_1 に検証鍵 svk をセットする ($C_1 = svk$)。

[0107] また、暗号化パラメータ生成部 23 は、第 1 乱数 $r \in \mathbb{Z}_p^*$ を生成して暗号文生成部 24 に送出する。

[0108] 暗号文生成部 24 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

C_4 を生成する（S T 2 2）。

[数5]

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

[0109] 具体的にはステップS T 2 2において、暗号化パラメータ生成部23は、再暗号化鍵生成装置30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、暗号文生成部24は、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、暗号文生成部24は、公開パラメータにおける生成元 u 、 v と、ステップS T 2 1で生成した検証鍵 $s v k$ 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。

[0110] ステップS T 2 2の終了後、暗号文生成部24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6]

$$\begin{aligned} &\hat{S} \text{とステップS T 2 1で生成した署名鍵 } s s k \text{ による使い捨て署名 } \sigma \text{ を} \\ &\text{次式に示すように生成する（S T 2 3）。} \\ &\sigma = \hat{S} (s s k, (C_3, C_4)) \end{aligned}$$

[0111] しかる後、暗号文生成部24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。

[0112] 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）。

[0113] 以上により、暗号化処理が完了する。

[0114] （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S T 3 1～S T 3 3に示すように実行される。

[0115] すなわち、再暗号化鍵生成装置30の通信部33は、制御部35に制御さ

れて、鍵生成装置 10 から公開された復号装置 50 の公開鍵 X_j 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 x_i 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。

[0116] 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 x_i と、一時データ記憶部 32 内の復号装置 50 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 (ST32)。

[数7]

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

[0117] 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)。

[0118] 以上により、再暗号化鍵生成処理が完了する。

[0119] (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 ST41 ~ ST43 に示すように実行される。

[0120] 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。

[0121] 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)。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8]

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

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

[0122] 再暗号化処理部44は、検証に成功すると、第2乱数 $t \in \mathbb{Z}_p^*$ を生成し、次式に示すように、第1、第2、第3及び第4再暗号化データ C_2' , C_2'' , C_2''' , C_{2V} を生成する (S T 4 2)。

[数9]

$$\begin{aligned} C_2' &= X_i^t \\ C_2'' &= R_{ij}^{1/t} = g^{(x_j/x_i)^{t-1}} \\ C_2''' &= C_2^t = X_i^{rt} \\ C_{2V} &= g^t \end{aligned}$$

[0123] 具体的にはステップS T 4 2において、再暗号化処理部44は、再暗号化鍵生成装置30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、再暗号化処理部44は、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、再暗号化処理部44は、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。さらに、再暗号化処理部44は、第2乱数 t を用いて、第4再暗号化データ C_{2V} を生成する。

[0124] ステップS T 4 2の終了後、再暗号化処理部44は、これら第1乃至第4再暗号化データ $C_2' \sim C_2''', C_{2V}$ を、暗号文データ C_i 内の第2暗号化データ C_2 と置換して再暗号文データ $C_j = (C_1, C_2', C_2'', C_2''', C_{2V}, C_3, C_4, \sigma)$ を生成し、得られた暗号文データを一時データ記憶部42に書き込む。

[0125] 通信部43は、制御部47に制御されて一時データ記憶部42内の再暗号文データ C_j を復号装置50に送信する (S T 4 3)。

[0126] 以上により、再暗号化処理が完了する。

[0127] (5) 復号処理は、復号装置50により、図6及び以下のステップS T 5 1 ~ S T 5 4 に示すように実行され、ステップS T 5 4 が失敗した場合には更にステップS T 5 5, S T 5 6 が実行される。

[0128] すなわち、復号装置50の通信部53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 52 に書き込む。

[0129] 復号処理部 54 は、公開パラメータ及び自装置 50 の公開鍵 X_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)。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10]

$$\begin{aligned} e(C'_2, C''_2) &\stackrel{?}{=} e(X_j, g) \\ e(C''_2, u^{C_1} \cdot v) &\stackrel{?}{=} e(C'_2, C_4) \\ \hat{V}(C_1, \sigma, (C_3, C_4)) &\stackrel{?}{=} 1 \end{aligned}$$

[0130] 復号処理部 54 は、検証に成功すると、自装置の秘密鍵 x_j に基づいて、次式に示すように、再暗号文データ C_j からメッセージ m を復号する (ST52)。

[数11]

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

[0131] 一方、通信部 53 は、制御部 56 に制御され、鍵生成装置 10 から公開された再暗号化鍵生成装置 30 の公開鍵 X_i を取得して一時データ記憶部 52 に書き込む。ここで、再暗号化鍵生成装置 30 の公開鍵 X_i は、再暗号文データ C_j が再暗号化处理される前の暗号文データ C_i の宛先と思われる識別情報 i をもつ装置の公開鍵 X_i に相当する。

[0132] 暗号文検証処理部 55 は、再暗号化システムに用いられる再暗号文データ C_j の一部と、当該再暗号文データ C_j を再暗号化处理する前の暗号文データ C_i の暗号化处理に用いられた公開鍵 X_i が代入された場合に成立する次式の如き検証式を予め保持している。

[数12]

$$e(C'_2, g) = e(C_{2V}, X_i)$$

なお、この検証式の左辺と右辺は次のように表すことができる。

$$(\text{検証式の左辺}) = e(g^{x_{r'}}, g) = e(g, g)^{x_{r'}}$$

$$(\text{検証式の右辺}) = e(g^t, g^{x_i}) = e(g, g)^{x_{r'}}$$

[0133] 続いて、暗号文検証処理部55は、前述した検証式に基づき、再暗号化装置40から受けた再暗号文データ C_j の一部(C'_2 , C_{2V})と、一時データ記憶部52から読み出した再暗号化鍵生成装置30の公開鍵 X_i を当該検証式に代入して演算を実行することにより、この検証式が成立するか否かを判定して再暗号文データが元々誰宛の暗号文だったかを検証する(ST54)。

[0134] 暗号文検証処理部55は、この判定の結果、検証式が成立したとき、平文データとしてのメッセージ m の暗号化処理に用いられた公開鍵が再暗号化鍵生成装置30の公開鍵 X_i であった旨を示す検証成功を出力する。

[0135] また、ステップST54の判定の結果、検証式が成立しないとき、新たに別の装置(例、図示しない他の再暗号化装置)の公開鍵を取得し(ST55)、ステップST54と同様の検証を繰り返すことにより(ST56)、検証式が成立する公開鍵をもつ再暗号化装置を特定する。

[0136] 上述したように本実施形態によれば、再暗号文データ C_j の一部と、当該再暗号文データ C_j を再暗号化処理する前の暗号文データ C_i の暗号化処理に用いられた公開鍵 X_i と、当該再暗号文データ C_j を復号可能な秘密鍵 x_j とが代入された場合に成立する検証式を予め保持して当該検証式を検証する暗号文検証処理部55を復号装置50が備えた構成により、再暗号文データを受けた復号装置が、元々誰宛の暗号文データが再暗号化されたのかを検証することができる。

[0137] 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。

[0138] また、本実施形態は、非特許文献 8 にあ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、メッセージ m は、復号装置 50 ではなく、再暗号化鍵生成装置 30 が有する秘密鍵 x_i により復号される。例えば、再暗号化鍵生成装置 30 は、ステップ S T 4 1 と同様に暗号文データを検証した後、次式に基づいて、メッセージ m を復号する。

[数13]

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

[0139] すなわち、本実施形態の再暗号化システムにおいて、非特許文献 8 に記載の技術に、再暗号化処理部 44 で C_{2v} を生成する処理および暗号文検証処理部 55 を付加すると実施することができる。

[0140] これに加え、本実施形態では、再暗号化鍵生成装置 30 が再暗号化処理を実行せずに暗号文データを復号する場合でも、次式に示すように暗号文データを検証すると、元々暗号文データに用いられていた公開鍵が、自身の装置（再暗号化鍵生成装置 30）の公開鍵 X_i であることを確認することができる。

[数14]

$$e(C'_2, g) = e(C_{2v}, X_i)$$

なお、上式の左辺と右辺は次のように表すことができる。

$$(\text{上式の左辺}) = e(g^{x_{r'}}, g) = e(g, g)^{x_{r'}}$$

$$(\text{上式の右辺}) = e(g^t, g^{x_i}) = e(g, g)^{x_i \cdot t}$$

[0141] （第 2 の実施形態）

次に、第 2 の実施形態に係る再暗号化システムについて、前述した図 1 を用いて説明する。本実施形態は、第 1 の実施形態の変形例であり、予めメッセージ m に再暗号化鍵生成装置 30 の公開鍵 X_i を埋め込んでおく構成により

、任意の再暗号化システムにおいて、元々誰宛の暗号文データであったかを検証可能にしたものである。

[0142] 具体的には、暗号化装置 20 の暗号文生成部 24 は、再暗号化鍵生成装置 30 の公開鍵 X_i を平文データとしてのメッセージ m に埋め込むと、当該埋め込み済みのメッセージ m に対して、前述した暗号化処理を実行する機能をもっている。ここで、埋め込む処理としては、例えば、電子透かしの生成処理を用いてもよく、あるいは単に、メッセージ m に公開鍵 X_i 又は公開鍵 X_i の暗号文を追加（連結）する処理を用いてもよい。公開鍵 X_i の暗号文は、例えば、暗号文生成部 24 が自装置 20 の秘密鍵 x_h で再暗号化鍵生成装置 30 の公開鍵 X_i を暗号化して作成された場合には、復号装置 50 において、暗号化装置 20 の公開鍵 X_h で復号されることにより、再暗号化鍵生成装置 30 の公開鍵 X_i が抽出可能となっている。

[0143] これに伴い、暗号化装置 20 の制御部 25 は、図 7 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。

[0144] 一方、復号装置 50 の暗号文検証処理部 55 は、前述した保持機能 (f55-1)、判定機能 (f55-2) 及び出力機能 (f55-3) に代えて、以下の各機能 (f55-4)～(f55-6) をもっている。

[0145] (f55-4) 前述した復号機能により復号されたメッセージ m から埋め込まれた公開鍵 X_i を抽出する抽出機能。

[0146] (f55-5) 当該抽出された公開鍵 X_i と、一時データ記憶部 52 から読み出した再暗号化鍵生成装置 30 の公開鍵 X_i とを比較する比較機能。

[0147] (f55-6) この比較の結果、両者が一致したとき、メッセージ m の暗号化処理に用いられた公開鍵 X_i が再暗号化鍵生成装置 30 の公開鍵 X_i であった旨を示す検証成功を出力する機能。

[0148] これに伴い、復号装置 50 の制御部 56 は、図 8 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。

[0149] 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 7 及び図 8 のシーケンス図を用いて説明する。

- [0150] (1) 鍵セットアップ処理の動作は、前述した通りである。
- [0151] (2) 暗号化処理のステップST21の動作は、前述した通りである。
- [0152] ステップST21の終了後、暗号化装置20の暗号文生成部24は、図7に示すように、再暗号化鍵生成装置30の公開鍵 X_i を平文データとしてのメッセージ m に埋め込む(ST22-x)と、当該埋め込み済みのメッセージ m に対して、前述したステップST22の動作を実行する。
- [0153] すなわち、暗号文生成部24は、第1乱数 r に基づき、当該埋め込み済みのメッセージ $m \in G_T$ に対して、前述した通り、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(ST22)。
- [0154] 暗号化処理のステップST23～ST24の動作は、前述した通りである。
- [0155] (3) 再暗号化鍵生成処理及び(4)再暗号化処理の動作は、前述した通りである。
- [0156] (5) 復号処理のステップST51～ST53の動作は、前述した通りである。
- [0157] ステップST53の終了後、復号装置50の暗号文検証処理部55は、図8に示すように、復号されたメッセージ m から埋め込まれた公開鍵 X_i を抽出する(ST54-x1)。
- [0158] 暗号文検証処理部55は、当該抽出された公開鍵 X_i と、一時データ記憶部52から読み出した再暗号化鍵生成装置30の公開鍵 X_i とを比較することにより、再暗号文データが元々誰宛の暗号文だったかを検証する(ST54-x2)。
- [0159] 暗号文検証処理部55は、この比較の結果、両者が一致したとき、メッセージ m の暗号化処理に用いられた公開鍵 X_i が再暗号化鍵生成装置30の公開鍵 X_i であった旨を示す検証成功を出力する。
- [0160] また、ステップST54-x2の判定の結果、両者が一致しないとき、新たに別の装置(例、図示しない他の再暗号化装置)の公開鍵を取得して(ST55-x)一時データ記憶部52に書き込み、ステップST54-x2と

同様の検証を繰り返すことにより（ST56-x）、抽出された公開鍵に一致する公開鍵をもつ再暗号化装置を特定する。

[0161] 上述したように本実施形態によれば、暗号化装置20は、再暗号化鍵生成装置30の公開鍵 X_i を平文データとしてのメッセージ m に埋め込むと、当該埋め込み済みのメッセージ m に対して、前述した暗号化処理を実行する暗号文生成部24を備えている。また、復号装置50は、復号されたメッセージ m から埋め込まれた公開鍵 X_i を抽出して当該公開鍵 X_i と、一時データ記憶部52から読み出した再暗号化鍵生成装置30の公開鍵 X_i とを比較して検証する暗号文検証処理部55を備えている。従って、本実施形態では、このような暗号化装置20及び復号装置50を備えた構成により、再暗号文データを受けた復号装置が、元々誰宛の暗号文データが再暗号化されたのかを検証することができる。

[0162] 以上説明した少なくとも一つの実施形態によれば、再暗号化システムにおいて、再暗号文データを受けた復号装置が、元々誰宛の暗号文データが再暗号化されたのかを検証することができる。

[0163] 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。

[0164] 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。

[0165] 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。

[0166] 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。

[0167] 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。

[0168] 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。

[0169] 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。

[0170] 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]

暗号化装置（20）が再暗号化鍵生成装置（30）の秘密鍵に対応する公開鍵を用いて平文データを暗号化処理して得られた暗号文データを再暗号化装置（40）に送信し、前記再暗号化装置がこの暗号文データを復号せずに再暗号化鍵により再暗号化処理して得られた再暗号文データを復号装置（50）に送信し、前記復号装置が前記再暗号化装置の公開鍵を用いて前記再暗号文データを検証処理すると共に、前記復号装置が自己の公開鍵に対応する秘密鍵を用いて前記再暗号文データを復号処理して前記平文データを得る再暗号化システムにおいて、前記再暗号化鍵生成装置の公開鍵と前記復号装置の秘密鍵を記憶する記憶手段を備えた前記復号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可能な記憶媒体（M5）に記憶された再暗号文検証プログラムであって、

前記再暗号化システムに用いられる再暗号文データの一部と、当該再暗号文データを再暗号化処理する前の暗号文データの暗号化処理に用いられた公開鍵が代入された場合に成立する検証式が予め記述されたプログラムコードを保持する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（55）、

前記検証式に基づき、前記再暗号化装置から受けた再暗号文データの一部と、前記記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵を当該検証式に代入して演算を実行することにより、この検証式が成立するか否かを判定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（55）、

この判定の結果、前記検証式が成立したとき、前記平文データの暗号化処理に用いられた公開鍵が前記再暗号化鍵生成装置の公開鍵であった旨を示す検証成功を出力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（55）、

を備えた再暗号文検証プログラム。

[請求項2]

請求項1に記載の再暗号文検証プログラムにおいて、

前記再暗号化鍵生成装置の秘密鍵及び公開鍵をそれぞれ x_i 及び X_i で表し（但し、セキュリティパラメータ λ に基づき、素数位数 $p > 2^\lambda$ を満たす双線型写像群を G , G_T で表し、第1生成元を $g \in G$ で表したとき、

公開パラメータ $(p, \lambda, G, G_T, g, u, v, \text{Sig})$ 、

前記平文データを $m \in G_T$ で表し、

前記暗号文データを $C_i = (C_1, C_2, C_3, C_4, \sigma)$ で表し（但し、使い捨て署名の署名鍵及び検証鍵をそれぞれ $s s k$ 及び $s v k$ で表し、素数 p に対する乗法群を Z_p^* で表し、第1乱数を $r \in Z_p^*$ で表し、ペアリング関数を $e(,)$ で表し、第2及び第3生成元をそれぞれ $u, v \in G$ で表し、前記使い捨て署名の署名生成機能を

[数1]

$\hat{S}$ で表したとき、

$$C_1 = s v k,$$

$$C_2 = X_i^r$$

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

$$C_4 = (u^{svk} \cdot v)^r$$

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

)、

前記復号装置の秘密鍵及び公開鍵をそれぞれ x_j 及び X_j で表し（但し、

[数2]

$$X_i = g^{x_i}$$

$$X_j = g^{x_j}$$

)、

前記再暗号化鍵を

[数3]

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

で表し、

前記再暗号文データを $C_j = (C_1, C_2', C_2'', C_2''', C_{2v}, C_3, C_4, \sigma)$ で表すとき（但し、第2乱数を $t \in Z_p^*$ で表したとき、

[数4]

$$\begin{aligned} C_2' &= X_i^t \\ C_2'' &= R_{ij}^{1/t} = g^{(x_j/x_i)^{t-1}} \\ C_2''' &= C_2' = X_i^{t^2} \\ C_{2v} &= g^t \end{aligned}$$

)、

前記検証式は、

[数5]

$$e(C_2', g) = e(C_{2v}, X_i)$$

で表されることを特徴とする再暗号文検証プログラム。

[請求項3]

請求項1又は請求項2に記載の再暗号文検証プログラムを用いた前記再暗号化装置(40)において、

前記再暗号文検証プログラムを記憶する検証プログラム記憶手段(45)と、

この再暗号文検証プログラムの配信要求を前記復号装置から受けると、前記検証プログラム記憶手段内の再暗号文検証プログラムを当該復号装置に配信する検証プログラム配信手段(46)と、

を備えた再暗号化装置。

[請求項4]

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）を備えた再暗号化システムであって、前記暗号化装置（20）は、

前記再暗号化鍵生成装置の公開鍵を記憶する第1記憶手段（21）と、

前記第1記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵を用いて前記平文データを暗号化処理することにより、暗号文データを得る暗号化手段（24）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手段（22）と、

を備え、

前記再暗号化鍵生成装置（30）は、

前記再暗号化鍵生成装置の公開鍵に対応する秘密鍵と、前記復号装置の秘密鍵に対応する公開鍵とを記憶する第2記憶手段（31、32）と、

前記第2記憶手段から読み出した前記再暗号化鍵生成装置の秘密鍵と前記復号装置の公開鍵とを用いて再暗号化鍵を生成する手段（34）と、

前記生成された再暗号化鍵を前記再暗号化装置に送信する手段（33）と、

を備え、

前記再暗号化装置（40）は、

前記再暗号化鍵生成装置から受けた再暗号化鍵を記憶する第3記憶手段（41）と、

前記暗号化装置から暗号文データを受けると、前記第3記憶手段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処理することにより、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復号装置に送信する手段 (43)

) と、

を備え、

前記復号装置 (50) は、

前記再暗号化鍵生成装置の公開鍵と前記復号装置の秘密鍵を記憶する第4記憶手段 (51, 52) と、

前記再暗号化装置から再暗号文データを受けると、前記第4記憶手段から読み出した当該復号装置の秘密鍵に基づいて、当該再暗号文データを復号処理することにより、前記平文データを得る復号手段 (54) と、

前記再暗号化システムに用いられる再暗号文データの一部と、当該再暗号文データを再暗号化処理する前の暗号文データの暗号化処理に用いられた公開鍵が代入された場合に成立する検証式を予め保持する保持手段 (55) と、

前記保持手段から読み出した検証式に基づき、前記再暗号化装置から受けた再暗号文データの一部と、前記第4記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵を当該検証式に代入して演算を実行することにより、この検証式が成立するか否かを判定する判定手段 (55) と、

この判定の結果、前記検証式が成立したとき、前記平文データの暗号化処理に用いられた公開鍵が前記再暗号化鍵生成装置の公開鍵であった旨を示す検証成功を出力する出力手段 (55) と、

を備えたことを特徴とする再暗号化システム。

[請求項5]

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) を備えた再暗号化システムであって、前記暗号化装置 (20) は、

前記再暗号化鍵生成装置の公開鍵を記憶する第1記憶手段 (21)

と、

前記再暗号化装置の公開鍵を前記平文データに埋め込むと、当該埋め込み済みの平文データを、前記第 1 記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵に基づいて暗号化处理することにより、暗号文データを得る暗号化手段（24）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手段（22）と、

を備え、

前記再暗号化鍵生成装置（30）は、

前記再暗号化鍵生成装置の公開鍵に対応する秘密鍵と、前記復号装置の秘密鍵に対応する公開鍵とを記憶する第 2 記憶手段（31、32）と、

前記第 2 記憶手段から読み出した前記再暗号化鍵生成装置の秘密鍵と前記復号装置の公開鍵とを用いて再暗号化鍵を生成する手段（34）と、

前記生成された再暗号化鍵を前記再暗号化装置に送信する手段（33）と、

を備え、

前記再暗号化装置（40）は、

前記再暗号化鍵生成装置から受けた再暗号化鍵を記憶する第 3 記憶手段（41）と、

前記暗号化装置から暗号文データを受けると、前記第 3 記憶手段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处理することにより、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復号装置に送信する手段（43）と、

を備え、

前記復号装置（５０）は、

前記再暗号化鍵生成装置の公開鍵と前記復号装置の秘密鍵を記憶する第４記憶手段（５１，５２）と、

前記再暗号化装置から再暗号文データを受けると、前記第４記憶手段から読み出した当該復号装置の秘密鍵に基づいて、当該再暗号文データを復号処理することにより、前記平文データを得る復号手段（５４）と、

前記復号手段により復号された平文データから前記埋め込まれた公開鍵を抽出する抽出手段（５５）と、

前記抽出された公開鍵と、前記第４記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵とを比較する比較手段（５５）と、

この比較の結果、両者が一致したとき、前記平文データの暗号化処理に用いられた公開鍵が前記再暗号化鍵生成装置の公開鍵であった旨を示す検証成功を出力する手段（５５）と、

を備えたことを特徴とする再暗号化システム。

[請求項６]

請求項４又は請求項５に記載の再暗号化システムにおいて、

前記再暗号化装置及び復号装置のそれぞれの公開鍵と秘密鍵のペアを生成する鍵生成装置（１０）を更に備えたことを特徴とする再暗号化システム。