

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 3 月 6 日(06.03.2014)



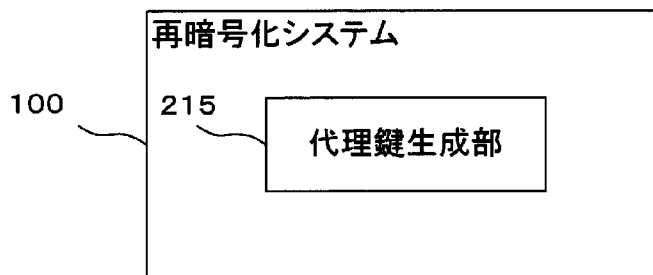
(10) 国際公開番号

WO 2014/034018 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) G06F 21/62 (2013.01)
- (21) 国際出願番号: PCT/JP2013/004576
- (22) 国際出願日: 2013 年 7 月 29 日(29.07.2013)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2012-189548 2012 年 8 月 30 日(30.08.2012) JP
- (71) 出願人: 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号 Tokyo (JP).
- (72) 発明者: 古川 潤(FURUKAWA, Jun); 〒1088001 東京都港区芝五丁目 7 番 1 号日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 岩壁 冬樹, 外(IWAKABE, Fuyuki et al.); 〒1040031 東京都中央区京橋二丁目 8 番 7 号 読売中公ビル 6 階 サンライズ国際特許事務所 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告 (条約第 21 条(3))

(54) Title: RE-ENCRYPTION SYSTEM, RE-ENCRYPTION METHOD AND RE-ENCRYPTION PROGRAM

(54) 発明の名称: 再暗号化システム、再暗号化方法および再暗号化プログラム



100 Re-encryption system

215 Proxy key generation unit

(57) Abstract: The objective of the present invention is to provide a re-encryption system capable of facilitating access control to data. The re-encryption system (100) is provided with a proxy key generation unit (215) which receives as input a master key possessed by a manager, a set of persons capable of decryption before modification, and a set of persons capable of decryption after modification, and generates and outputs a proxy key for converting cipher-text capable of being decrypted with a secret key of a decryptor belonging to the set of persons capable of decryption before modification to new cipher-text capable of being decrypted with a secret key of a decryptor belonging to the set of persons capable of decryption after modification.

(57) 要約: データへのアクセス制御を容易にすることができる再暗号化システムを提供することを目的とする。再暗号化システム 100 は、管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する代理鍵生成部 215 を備える。



WO 2014/034018 A1

明 細 書

発明の名称：

再暗号化システム、再暗号化方法および再暗号化プログラム

技術分野

[0001] 本発明は、複数の受信者が復号できる放送型暗号文を変換する放送型暗号の再暗号化システム、再暗号化方法および再暗号化プログラムに関し、この変換が対象となる暗号文を復号できる受信者の集合を変更する技術に関する。

背景技術

[0002] 放送型暗号方式は、同一の暗号文を、それぞれ異なる秘密鍵を持った複数の受信者が受信し、それぞれ復号した結果が同じ平文となる暗号方式である。一般的な放送型暗号方式として、例えば、非特許文献１にあげられる暗号方式がある。図６は、一般的な放送型暗号方式を用いた放送型暗号システムを示すブロック図である。図６に示す放送型暗号化システムは、設定部１１５と、鍵導出部１０７と、暗号化部１０６と、復号部１１３とを備える。

[0003] 設定部１１５は、公開鍵１０１およびマスター鍵１０５を生成する。暗号化部１０６は、公開鍵１０１と、復号可能者の集合を指定するデータである復号可能者集合１０３と、文書１０２とを用いて、暗号文１０９を生成する。鍵導出部１０７は、マスター鍵１０５と、公開鍵１０１と、復号者識別子１０４とを用いて、復号者秘密鍵１１２を生成する。復号部１１３は、公開鍵１０１と、暗号文１０９と、復号可能者の集合を指定するデータである復号可能者集合１１０と、復号者秘密鍵１１１とを用いて、暗号文１０９を復号した結果である文書１１４を生成する。

[0004] 図６に示す放送型暗号システムにおいて、暗号化部１０６が入力した復号可能者集合１０３と復号部１１３が入力した復号可能者集合１１０を指定するデータが同一であり、暗号化部１０６が出力した暗号文１０９と復号部１１３が入力した暗号文１０９が同一であり、復号部１１３が入力した復号者

秘密鍵 1 1 1 が、復号部 1 1 3 が入力した復号可能者集合 1 1 0 に指定される復号可能者の集合に属する復号者の秘密鍵であるならば、暗号化部 1 0 6 が入力した文書 1 0 2 と、復号部 1 1 3 が出力する文書 1 1 4 は同一となる。

[0005] このような放送型暗号方式は、クラウド等を利用したデータ保存サービスにおいてその安全性を高めることに寄与する。例えば、企業等のある組織がクラウド等にデータを保存する場合、この組織のメンバーのみが読めるべきデータが、上記放送型暗号方式を用いて暗号化されてクラウド等に保存される。組織のメンバーは、復号可能者集合 1 0 3 に属し、各自対応する秘密鍵を渡される。組織のメンバーは、データを必要とするときにクラウド等にアクセスし、必要なデータを取り寄せる。このデータは暗号化されているが、組織のメンバーであれば上記放送型暗号方式の復号方式に従い復号し、利用することができる。

[0006] クラウド等の認証システムは、データの取り寄せ要求に対して、認証を行いアクセス可能な者を対応する組織のメンバーに限ることで、適切なアクセス制御を実施することができるが、アクセス制御にミスが発生する可能性がある。または、クラウド等の管理が不十分であったり、クラウド等の管理者が不正を働きアクセス権限を持たない者がデータを手に入ってしまったりする可能性もある。また、外部の利用者が、クラウド等の管理が十分であることを確認することや、クラウド等の管理者が不正を働かない確証を得ることは難しい。しかし、上記放送型暗号方式を用いると、上記組織のメンバー以外がデータを手に入れることに成功しても、データを復号することができないため、その内容が組織外に明らかになることは防がれる。

[0007] さらに、上記放送型暗号方式を用いることの利点は、ある時点でメンバーの変更があったときに復号可能者集合を変更できるところにある。新しいメンバーが組織に加わった場合は、鍵導出部 1 0 7 が復号者秘密鍵 1 1 2 を生成してこのメンバーに付与し、復号可能者集合にこのメンバーを追加する。その上で、以降のデータ保存においては新しい復号可能者集合を用いてデー

タを暗号化する。逆にあるメンバーが組織から去ったときには、復号可能者集合からこのメンバーを削除する。その上で、以降のデータ保存においては新しい復号可能者集合を用いてデータを暗号化する。これらの処理により、新しく保存されるデータに関しては、更新された復号可能者集合に属する最新のメンバーのみが復号できるようになる。

先行技術文献

非特許文献

- [0008] 非特許文献1: DanBoneh, CraigGentry, BrentWaters” CollusionResistantBroadcastEncryptionWithShortCiphertextsandPrivateKeys” , AdvancesinCryptography-CRYPT02005:25thAnnualInternationalCryptographyConference, SantaBarbara, California, USA, August14-18, 2005, Proceedings. LectureNotesinComputerScience3621Springer2005, ISBN3-540-28114-2, pp.258-275.

発明の概要

発明が解決しようとする課題

- [0009] 非特許文献1に示すような放送型暗号方式を用いたデータ保存サービスにおいては、メンバーの追加や抹消等の事象が発生した場合、復号可能者集合を変更することで、新たに保存されるデータへのアクセス制限を更新することが可能である。その一方、既に保存されていたデータの復号に対するアクセス制限を更新することができない。なぜなら、既に保存されているデータを誰が復号できるかはそのデータが暗号化される時に定まり、その後は変更されないからである。
- [0010] このような問題への対応策として、組織を構成するメンバーが変わったときには全ての保存されるデータを一旦取り出し、古い復号可能者集合を用いて全て復号し、新しい復号可能者集合を用いて暗号化し、再度保存することが考えられる。しかし、多くの一般的な組織、特に大きな組織では、その構成メンバーの変更は頻繁に行われるので、上記のような取り出しと復号と暗号化とが伴う処理をメンバー変更の度に行うと、極めてシステムの負担が大

きくなる。すなわち、クラウド等を用いたデータ保存サービス等のサービスにおいてそのアクセス制御を非特許文献 1 に示すような一般的な放送型暗号方式に依存することは多くの組織にとって実用的ではない。

[0011] そこで、本発明は、データへのアクセス制御を容易にすることができる再暗号化システム、再暗号化方法および再暗号化プログラムを提供することを目的とする。

課題を解決するための手段

[0012] 本発明による再暗号化システムは、管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する代理鍵生成部を備えたことを特徴とする。

[0013] 本発明による再暗号化方法は、管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力することを特徴とする。

[0014] 本発明による再暗号化プログラムは、コンピュータに、管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する代理鍵生成処理を実行させることを特徴とする。

発明の効果

[0015] 本発明によれば、データへのアクセス制御を容易にすることができる。

図面の簡単な説明

[0016] [図1]本発明による再暗号化システムの第 1 の実施形態および第 2 の実施形態の構成を示すブロック図である。

[図2]本発明による再暗号化システムの第1の実施形態および第2の実施形態の動作の例を示すフローチャートである。

[図3]本発明による再暗号化システムの第3の実施形態の構成を示すブロック図である。

[図4]本発明による再暗号化システムの第3の実施形態の動作の例を示すフローチャートである。

[図5]本発明による再暗号化システムの主要部を示すブロック図である。

[図6]一般的な放送型暗号方式を用いた放送型暗号システムを示すブロック図である。

発明を実施するための形態

[0017] 以下の説明において、群1と群2は、位数を q とした巡回群とする。また、双線型写像 $e: \text{群1} \times \text{群1} \rightarrow \text{群2}$ が存在するものとし、 F_q を標数 q の素体とする。群1は、加法巡回群として記述される。 F_q の元と群1の元には乗算が定義されており、 F_q の元が α であり、群1の元が G ならばそれらの乗算は αG と記述される。群2の元は乗法巡回群として記述される。 F_q の元と群2の元には冪乗算が定義されており、 F_q の元が α で群1の元が g ならばそれらの冪乗算は g^α と記述される。群1や群2の実現方法として、楕円曲線を用いた方法などが知られている。

[0018] 実施形態1.

図1は、本発明による再暗号化システムの第1の実施形態（実施形態1）の構成を示すブロック図である。本実施形態の再暗号化システムは、設定部220と、鍵導出部207と、暗号化部206と、再暗号化装置200と、復号部213とを備える。再暗号化装置200は、代理鍵生成部215と、再暗号化部221と、鍵更新部219とを含む。本実施形態の再暗号化システムは、例えば、特定の演算処理等を行うよう設計されたハードウェア、またはプログラムに従って動作するCPU（Central Processing Unit）等の情報処理装置によって実現される。

[0019] 設定部220は、潜在的な復号者数を表す整数 L を入力する。また、設定

部220は、群1および群2を、位数 q の巡回群として、双線型写像 $e: \text{群}1 \times \text{群}1 \rightarrow \text{群}2$ が存在するものから選ぶ。また、 F_q を標数 q の素体とする。設定部220は、群1の生成元 G を選び、 α 、 γ を F_q からランダムに選ぶ。設定部220は、 $g_T = e(G, G)$ 、 $(G[i])_{i=1, \dots, L, L+2, \dots, 2L} = (\alpha^i G)_{i=1, \dots, L, L+2, \dots, 2L}$ 、 $F = \gamma G$ を生成する。そして、設定部220は、公開鍵201として $pk = (q, G, G_T, e(), G, (G[i])_{i=1, \dots, L, L+2, \dots, 2L}, F)$ を出力し、マスター鍵205として $mk := (\alpha, \gamma)$ を出力する。マスター鍵は、データへのアクセス権を有する者が持つことができる鍵である。

[0020] 鍵導出部207は、公開鍵201 (pk)、マスター鍵205 (mk)、復号者識別子204 (k)を入力する。そして、鍵導出部207は、復号者識別子が k である復号者の秘密鍵212として $s_k[k] = D[k] = \gamma G[k]$ を出力する。

[0021] 暗号化部206は、公開鍵201 (pk)、復号可能者集合203 (S)、文書202を入力し、 τ を F_q からランダムに選ぶ。また、暗号化部206は、 $h = e(G[1], G[L])^\tau$ 、 $C[0] = \tau G$ 、 $C[1] = \tau(F + \sum_{i \in S} G[L+1-i])$ を生成する。また、暗号化部206は、ヘッダ $hdr = h$ を共通鍵として文書を暗号化したものを、 $C[2]$ とし、暗号文209として、 $ct = (C[0], C[1], C[2])$ を出力する。

[0022] 代理鍵生成部215は、公開鍵201 (pk)、マスター鍵205 ($mk := (\alpha, \gamma)$)、現在の復号可能者集合203 (S)、新しい復号可能者集合210 (S')を入力する。また、代理鍵生成部215は、 δ を F_q からランダムに選ぶ、 $F' = \delta G$ 、 $\rho = (\gamma + \delta + \sum_{i \in S'} \alpha^{L+1-i}) / (\gamma + \sum_{i \in S} \alpha^{L+1-i})$ 、 $(G'[i])_{i \in U} = (\delta G[i])_{i \in U}$ を生成する。ここで U は $\{1, \dots, L\}$ とする。代理鍵生成部215は、新しいマスター鍵として $mk' = (\alpha, \gamma + \delta)$ を出力し、代理鍵216として $rk = \rho$ を出力し、更新情報217として $(pk' = F', (uk[i])_{i \in U} = (G'[i])_{i \in U})$ を出力する。

[0023] 再暗号化部 221 は、暗号文 209 ($ct := (C[0], C[1], C[2])$) と代理鍵 216 ($rk = \rho$) とを入力する。再暗号化部 221 は、新しい暗号文 222 ($ct' = (C[0], \rho C[1], C[2])$) を出力する。

[0024] 鍵更新部 219 は、復号者識別子 204 (k) と、公開鍵 201 (pk) と、更新情報 217 の少なくとも一部 ($pk' = F'$, $u_k[k] = G'[i]$) と、識別子が k である復号者秘密鍵 218 ($sk[k] = D[k]$) とを入力する。また、鍵更新部 219 は、復号者の識別子が k である復号者秘密鍵 218 ($sk[k]$) を新しい復号者秘密鍵 211 ($D[k] + G'[k]$) に更新し、公開鍵 201 (pk) の要素 F を $F + F'$ に更新する。

[0025] 復号部 213 は、復号者識別子 204 (k)、公開鍵 201 (pk)、暗号文 209 または新しい暗号文 222 ($ct = (C[0], C[1], C[2])$)、復号可能者集合 203 または新しい復号可能者集合 210 (S または S')、復号者秘密鍵 218 または新しい復号者秘密鍵 211 ($sk[k] = D[k]$) を入力する。また、復号部 213 は、 $hdr = e(G[k], C[1]) / e(C[0], D[k] + \sum_{i \in S \setminus \{k\}} G[L+1-i+k])$ を計算し、 $C[2]$ を hdr で復号して文書 214 を得て出力する。

[0026] 本実施形態の再暗号化システムが正常に動作することは次の説明により示される。まず、再暗号化がなされない場合に、暗号化時に生成されるヘッダと、復号の出力するヘッダが等しいことは次の説明により示される。

[0027] hdr
 $= e(G[k], C[1]) / e(C[0], D[k] + \sum_{i \in S \setminus \{k\}} G[L+1-i+k])$
 $= e(G[k], \tau u(F + \sum_{i \in S} G[L+1-i])) / e(\tau G, \gamma G[k] + \sum_{i \in S \setminus \{k\}} G[L+1-i+k])$
 $= e(\tau G, G[L+1] + \alpha^k \gamma G + \sum_{i \in S \setminus \{k\}} G[L+1-i+k]) / e(\tau G, \alpha^k \gamma G + \sum_{i \in S \setminus \{k\}} G[L+1-i+k])$
 $= e(G[1], G[L+1])^\tau = h$

[0028] 再暗号化がなされた場合にも、暗号化により生成されるヘッダと、復号部 213 が出力するヘッダが等しいことが次のように分かる。更新された S' に関する $k \in S'$ と更新された s_k' [k] と更新された公開鍵を用いて、再暗号化された暗号文 c_t' は以下のように復号される。ここで、 $\gamma' = \gamma + \delta$ とする。

$$\begin{aligned}
 [0029] \quad hdr &= e(G[k], \rho C[1]) / e(C[0], D[k] + G'[k] \\
 &\quad + \prod_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &= e(G[k], \rho \tau(F + \sum_{i \in S} G[L+1-i])) / e(\tau G, \gamma G[k] \\
 &\quad + G'[k] + \sum_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &= e(G[k], \rho \tau(\gamma + \sum_{i \in S} \alpha^{L+1-i}) G) / e(\tau G, \gamma' G[k] \\
 &\quad + \sum_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &= e(G[k], \tau(\gamma' G + \sum_{i \in S'} \alpha^{L+1-i})) / e(\tau G, \gamma' G[k] \\
 &\quad + \sum_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &= e(\tau \alpha^k G, \gamma' G + \sum_{i \in S'} G[L+1-i]) / e(\tau G, \gamma' G[k] \\
 &\quad + \sum_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &= e(\tau G, G[L+1] + \alpha^k \gamma' G + \sum_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &\quad / e(\tau G, \alpha^k \gamma' G + \sum_{i \in S' \setminus \{k\}} G[L+1-i+k]) \\
 &= e(G[1], G[L])^\tau = h
 \end{aligned}$$

[0030] 次に、本実施形態の再暗号化システムの動作を説明する。図2は、本発明による再暗号化システムの第1の実施形態の動作の例を示すフローチャートである。なお、本実施形態の再暗号化システムの動作の順序は、以下の順序には限定されない。

[0031] 設定部220は、潜在的な復号者数を表す整数 L を入力する。そして、公開鍵201 (p_k) とマスター鍵205 (m_k) とを出力する (ステップS11)。そして、鍵導出部207は、公開鍵201 (p_k)、マスター鍵205 (m_k)、復号者識別子204 (k) を入力し、復号者識別子が k である復号者の秘密鍵212として $s_k[k] = D[k] = \gamma G[k]$ を出力する (ステップS12)。

- [0032] 暗号化部206は、公開鍵201 (p_k)、復号可能者集合203 (S)、文書202を入力し、ヘッダ $hdr = h$ を共通鍵として文書を暗号化したものを、 $C[2]$ として、暗号文209 ($ct = (C[0], C[1], C[2])$) を出力する (ステップS13)。
- [0033] 代理鍵生成部215は、公開鍵201 (p_k)、マスター鍵205 ($mk := (\alpha, \gamma)$)、現在の復号可能者集合203 (S)、新しい復号可能者集合210 (S') を入力する。また、代理鍵生成部215は、新しいマスター鍵として $mk' = (\alpha, \gamma + \delta)$ を出力し、代理鍵216として $rk = \rho$ を出力し、更新情報217として ($pk' = F'$, $(u_k[i])_{i \in U} = (G'[i])_{i \in U}$) を出力する (ステップS14)。
- [0034] 再暗号化部221は、暗号文209 ($c := (C[0], C[1], C[2])$) と代理鍵216 ($rk = \rho$) とを入力し、新しい暗号文222として $ct' = (C[0], \rho C[1], C[2])$ を出力する (ステップS15)。
- [0035] 鍵更新部219は、復号者識別子204 (k) と、公開鍵201 (p_k) と、更新情報217の一部 ($pk' = F'$, $u_k[k] = G'[i]$) と、識別子が k の復号者秘密鍵218 ($sk[k] = D[k]$) とを入力し、復号者の識別子が k である復号者秘密鍵218 ($sk[k]$) を新しい復号者秘密鍵211 ($D[k] + G'[k]$) に更新する (ステップS16)。
- [0036] 復号部213は、復号者識別子204 (k)、公開鍵201 (p_k)、暗号文209または新しい暗号文222 ($ct = (C[0], C[1], C[2])$)、復号可能者集合203または新しい復号可能者集合210 (S または S')、復号者秘密鍵218または新しい復号者秘密鍵211 ($sk[k] = D[k]$) を入力し、 hdr を計算し、 $C[2]$ を hdr で復号して文書214を得て出力する (ステップS17)。
- [0037] 以上のように、本実施形態の再暗号化システムは、変更前の復号可能者の集合 S に属する復号者が復号できる暗号文を、変更後の復号可能者の集合 S' に属する復号者が復号できる暗号文に変更する (再暗号化する)。よって

、本実施形態の再暗号化システムは、データへのアクセス制御を動的に容易にすることができる。

[0038] 実施形態 2.

以下、第 2 の実施形態の再暗号化システムを説明する。本実施形態の再暗号化システムの構成および動作に関して特に説明しない部分は、図 1 および図 2 に示した第 1 の実施形態と同様であるため、説明は省略する。

[0039] 設定部 220 は、潜在的な復号者数を表す整数 L を入力する。群 1 および群 2 を、位数 q の巡回群として、双線型写像 $e : \text{群 1} \times \text{群 1} \rightarrow \text{群 2}$ が存在するものから選ぶ。また、 F_q を標数 q の素体とする。設定部 220 は、群 1 の生成元 G を選び、 α 、 $(\beta[b])_{b=1,2}$ 、 $(\gamma[b])_{b=1,2}$ を F_q からランダムに選ぶ。 b は、例えば 1 または 2 である。また、設定部 220 は、 $g_T = e(G, G)$ を生成し、 $(G[b])_{b=1,2} = (\{\beta[b]\} G)_{b=1,2}$ 、 $(F[b])_{b=1,2} = (\{\gamma[b]\} G)_{b=1,2}$ 、 $(G[b, i])_{b=1,2; i=1, \dots, L, L+2, \dots, 2L} = (\alpha^i G[b])_{i=1, \dots, L, L+2, \dots, 2L}$ を生成する。そして、設定部 220 は、公開鍵 201 として $pk = (q, G, G_T, e(), G, (G[b, i])_{b=1,2; i=1, \dots, L, L+2, \dots, 2L}, (G[b], F[b])_{b=1,2})$ を出力し、マスター鍵 205 として $mk := (\alpha, (\beta[b], \gamma[b])_{b=1,2})$ を出力する。

[0040] 鍵導出部 207 は、公開鍵 201 (pk)、マスター鍵 205 (mk)、復号者識別子 204 (k) を入力する。 $\eta[1, k]$ を F_q からランダムに選ぶ。なお、 $\eta[2, k] = ((\sum_{i=1,2} \beta[b] \gamma[b]) - \beta[1] \eta[1, k]) / \beta[2]$ である。識別子が k の復号者の秘密鍵 212 ($sk[k] = (D[b, k])_{b=1,2} = (\alpha^k \eta[b, k] G)_{b=1,2}$) を出力する。

[0041] 暗号化部 206 は、公開鍵 201 (pk)、復号可能者集合 203 (S)、文書 202 を入力する。 τ を F_q からランダムに選ぶ。また、暗号化部 206 は、 $h := \prod_{b=1,2} e(G[b, 1], G[b, L])^\tau$ 、 $(C[0, b])_{b=1,2} := (\tau G[b])_{b=1,2}$ 、 $(C[1, b])_{b=1,2} := (\tau (F[b] + \sum_{i \in S} G[b, L+1-i]))_{b=1,2}$ を生成する。また、暗号化部

206は、ヘッダ $hdr = h$ を共通鍵として文書を暗号化したものを、 $C[2]$ として、暗号文209として $ct = ((C[0, b], C[1, b])_{b=1, 2}, C[2])$ を出力する。

[0042] 代理鍵生成部215は、公開鍵201 (pk)、マスター鍵205 ($mk := (\alpha, (\beta[b], \gamma[b])_{b=1, 2})$)、現在の復号可能者集合203 (S)、新しい復号可能者集合210 (S') を入力する。また、代理鍵生成部215は、 $(\delta[b])_{b=1, 2}$ を F_q からランダムに選び、 $(F'[b])_{b=1, 2} = (\delta[b] G)_{b=1, 2}$ を生成し、 $(\rho[b])_{b=1, 2} = ((\gamma[b] + \delta[b] + \beta[b] (\sum_{i \in S'} \alpha^{L+1-i})) / (\gamma[b] + \beta[b] (\sum_{i \in S} \alpha^{L+1-i})))_{b=1, 2}$ を生成する。また、代理鍵生成部215は、 $(\eta'[1, i])_{i=1, \dots, L}$ を F_q からランダムに選び、 $(\eta'[2, i])_{i=1, \dots, L} = ((\sum_{b=1, 2} \beta[b] \delta[b]) - \beta[1] \eta'[1, i]) / \beta[2])_{i=1, \dots, L}$ を生成する。

[0043] また、代理鍵生成部215は、 $(G'[b, i])_{b=1, 2; i=1, \dots, L} = (\eta'[b, i] \alpha^i G)_{b=1, 2; i=1, \dots, L}$ を生成する。また、代理鍵生成部215は、新しいマスター鍵 ($mk' = (\alpha, (\beta[b], \gamma[b] + \delta[b])_{b=1, 2})$) を出力し、代理鍵216 ($rk = (\rho[b])_{b=1, 2}$) を出力し、更新情報217 ($F' = (F'[b])_{b=1, 2}, (uk[i])_{i=1, \dots, L} := ((G'[b, i])_{b=1, 2})_{i=1, \dots, L}$) を出力する。

[0044] 再暗号化部221は、暗号文209 ($ct := ((C[0, b], C[1, b])_{b=1, 2}, C[2])$)、代理鍵216 ($rk := (\rho[b])_{b=1, 2}$) を入力する。新しい暗号文222 ($ct' = (C[0, b], \rho[b] C[1, b])_{b=1, 2}$) を出力する。

[0045] 鍵更新部219は、復号者識別子204 (k) と、公開鍵201 (pk) と、更新情報217の一部 ($pk' = F' = (F'[b])_{b=1, 2}, uk[k] = (G'[b, k])_{b=1, 2}$) と、識別子が k である復号者秘密鍵218として ($sk[k] = (D[b, k])_{b=1, 2}$) を入力する。復号者の識別子が k である復号者秘密鍵218 ($sk[k]$) を新しい復号者秘密鍵211 (

$D[b, k] + G'[b, k])_{b=1, 2}$ に更新する。 p_k の要素($F[b]$)
 $b=1, 2$ を($F[b] + F'[b])_{b=1, 2}$ に更新する。

[0046] 復号部213は、復号者の識別子204(k)、公開鍵201(p_k)、
 暗号文209または新しい暗号文222($c_t = ((C[0, b], C[1, b])_{b=1, 2}, C[2])$)、復号者秘密鍵218または新しい復号者秘密
 鍵211($s_k[k] = (D[b, k])_{b=1, 2}$)を入力する。また、復号部
 213は、 $h = (\prod_{b=1, 2} e(G[b, k], C[1, b]) / (\prod_{b=1, 2} e(C[0, b], D[b, k] + \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k]))$
 を計算し、 $C[2]$ を $h d r$ で復号して文書214を得て出力する。

[0047] 本実施形態の再暗号化システムが正常に動作することは次のことから分か
 る。まず、再暗号化がなされない場合に、暗号化時に生成されるヘッダと、
 復号部213が出力するヘッダが等しいことは次のように分かる。ただし $A \wedge B$ は AB を表す。

[0048] $h = (\prod_{b=1, 2} e(G[b, k], C[1, b])) / (\prod_{b=1, 2} e(C[0, b], D[b, k] + \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k]))$
 $= (\prod_{b=1, 2} e(G[b, k], \tau(F[b] + \sum_{i \in S} G[b, L+1-i])) / (\prod_{b=1, 2} e(\tau G[b], \alpha^k \eta[b] G + \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k]))$
 $= (\prod_{b=1, 2} e(\tau G[b], G[b, L+1] + \alpha^k \gamma[b] G + \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k])) / (\prod_{b=1, 2} e(\tau G[b], \alpha^k \eta[b] G + \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k]))$
 $= (\prod_{b=1, 2} e(\tau G[b], G[b, L+1]) \prod_{b=1, 2} e(\tau G[b], \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k])) / (\prod_{b=1, 2} e(\tau G[b], \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k])) \cdot (e(G, G)^{\wedge (\tau \alpha^k \sum_{b=1, 2} \beta[b] \gamma[b])) / (e(G, G)^{\wedge (\tau \alpha^k \sum_{b=1, 2} \beta[b] \eta[b]))$
 $= \prod_{b=1, 2} e(G[b], G[b, L+1]) \tau$
 $= \prod_{b=1, 2} e(G[b], G[b])^{\wedge (\tau \alpha^{L+1})} = h$

[0049] 再暗号化がなされた場合にも、暗号化時に生成されるヘッダと、復号部 213 が出力するヘッダが等しいことが次のように分かる。更新された S' に関する $k \in S'$ と更新された s_k' [k] と更新された公開鍵を用いて、再暗号化された暗号文 c_t' は以下のように復号される。

$$\begin{aligned}
 [0050] \quad h &= (\prod_{b=1, 2} e(G[b, k], \rho[b] C[1, b])) / (\prod_{b=1, 2} e(C[0, b], D[b, k] + G'[b, k] \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k])) \\
 &= (\prod_{b=1, 2} e(G[b, k], \tau(F[b] + F'[b] + \sum_{i \in S} G[b, L+1-i])) / (\prod_{b=1, 2} e(\tau G[b], \alpha k (\eta[b, k] + \eta'[b, k]) G + \sum_{i \in S \setminus \{k\}} G[b, L+1-i+k])) \\
 &= \prod_{b=1, 2} e(G[b], G[b])^{\alpha^{L+1}} = h
 \end{aligned}$$

[0051] 以上のように、本実施形態の再暗号化システムは、変更前の復号可能者の集合 S に属する復号者が復号できる暗号文を、変更後の復号可能者の集合 S' に属する復号者が復号できる暗号文に変更する。よって、暗号文の復号可能者集合を変更することでデータへのアクセスを動的に容易に制御することができる。

[0052] 実施形態 3.

図 3 は、本発明による再暗号化システムの第 3 の実施形態の構成を示すブロック図である。以下で説明する、設定部 220、鍵導出部 207、暗号化部 206、代理鍵生成部 215、再暗号化部 221、鍵更新部 219、復号部 213 は、第 1 の実施形態に記述されたものと同じであるとする。

[0053] 本実施形態の再暗号化システムは、設定部 220 と鍵導出部 207 と代理鍵生成部 215 を含み管理者が操作する管理部 301 と、データの送受信部 321 と再暗号化部 221 を含み、暗号文を保存し、データ保存者によって操作されるデータ保存部 302 と、暗号文記憶部 322 とを備える。データ復号部 304 とデータ登録部 303 とは、本再暗号化システムの利用者によって操作される。データ登録部 303 は、暗号化部 206 を含み、データ復号部 304 は、鍵更新部 219 と復号部 213 を含む。復号者は、同時にデ

ータ登録者であってもよく、データ登録部303とデータ復号部304とは一つの構成であってもよい。

[0054] 管理部301は、設定部220を用いて公開鍵306とマスター鍵307を生成する。マスター鍵307は管理部301が保存し、管理者以外には明らかにされない。管理者は、データを読むことを許可する復号者を定めて、復号者の集合を復号可能者集合とする。管理部301は、各復号者に対して鍵導出部207を用いて秘密鍵308を生成して、データ復号部304に渡す。

[0055] データ登録者は、データ309の保存をデータ保存者に委託する場合、データ登録部303からデータ保存部302にアクセスして最新の公開鍵306を手に入れる。次に、データ登録部303の暗号化部206は、データ309を、暗号化してデータ保存部302に渡す。この時、暗号化部206は、復号可能者集合を指定して暗号化する。この指定がアクセス制御である。

[0056] 管理者が、暗号化データを復号できる復号可能者を増やすまたは減らす場合等、復号可能者集合を変更する場合、管理部301の代理鍵生成部215は、公開鍵201、古い復号可能者集合 S 、新しい復号可能者集合 S' およびマスター鍵307を用いて、代理鍵305 ($rk(S, S')$) を生成してデータ保存部302に送付する。この際、管理部301は、生成された鍵更新情報311もデータ保存部302に送付する。

[0057] データ保存部302の再暗号化部221は、代理鍵305 ($rk(S, S')$) を受け取ったら、保存している古い復号可能者集合 S を用いて暗号化された各暗号文を、再暗号化し、得られた新しい暗号文に入れ替える。この入れ替えにより、保存されている暗号文を復号できる復号者の集合が、新しい復号可能者集合 S' に変更される。また、公開鍵306も更新情報を用いて最新のものに更新される。

[0058] 復号者は、データ保存部302に保存されているデータを取り寄せたい場合、データ復号部304からデータ保存部302にアクセスする。この際、データ復号部304は、データ保存部302から新しい鍵更新情報311を

受け取ったら、復号者は、データ復号部304の鍵更新部219を用いて秘密鍵308を更新する。次に、復号者は、所望の暗号文データを取り寄せ、自身がこの暗号文の対応する復号可能者集合に属しているならば、更新された自身の秘密鍵308を用いて、復号部213により暗号文を復号してデータ310を得る。

[0059] 次に、本実施形態の再暗号化システムの動作を説明する。図4は、本発明による再暗号化システムの第3の実施形態の動作の例を示すフローチャートである。なお、本実施形態の再暗号化システムの動作の順序は、以下の順序には限定されない。

[0060] 管理部301は、設定部220を用いて公開鍵306とマスター鍵307を生成する（ステップS21）。管理部301は、各復号者に対して鍵導出部207を用いて秘密鍵308を生成して、データ復号部304に渡す（ステップS22）。

[0061] データ登録者が、データ309をデータ保存者に保存を委託する場合の動作を説明する。データ登録部303の暗号化部206は、データを暗号化してデータ保存部302に渡す（ステップS23）。

[0062] 管理者が、暗号化データを復号できる復号可能者を増やすあるいは減らす等、復号可能者集合を変更する場合、管理部301の代理鍵生成部215は、古い復号可能者集合S、新しい復号可能者集合S' およびマスター鍵307を用いて、代理鍵305（ $rk(S, S')$ ）を生成して、これをデータ保存部302に送付する（ステップS24）。

[0063] データ保存部302の再暗号化部221は、代理鍵305（ $rk(S, S')$ ）を受け取ったら、保存している古い復号可能者集合Sを用いて暗号化された各暗号文を、再暗号化し、得られた新しい暗号文に入れ替える（ステップS25）。

[0064] 復号者が、データ保存部302に保存されているデータを取り寄せたい場合の動作を説明する。まず、復号者は、データ保存部302にアクセスし、データ復号部304の鍵更新部219を用いて秘密鍵308を更新する（ス

テップ S 2 6)。次に、復号者は、所望の暗号文データを取り寄せ、自身がこの暗号文の対応する復号可能者集合に属しているならば、更新された自身の秘密鍵 3 0 8 を用いて、復号部 2 1 3 により暗号文を復号する（ステップ S 2 7）。

[0065] 以上に説明したように、本実施形態の再暗号化システムは、ある組織がクラウド等の外部で提供されるデータ保存サービスを利用しようとした際、データを暗号化してから保存する。そのため、本実施形態の再暗号化システムは、そのサービスからデータが漏洩することを恐れる可能性や、そのサービスの管理者がデータを閲覧する可能性を容易に軽減することができる。

[0066] 特に、本実施形態の再暗号化システムは、データを復号できる者の集合を変更することで、例えば企業等のメンバーが変更された場合に変更されたメンバーに対するデータへのアクセス制御を可能にする。多くのデータ保存サービスにおけるアクセス制御は、アクセス権限の変更が可能であることが求められている。この様な求めに対して、本実施形態の再暗号化システムは、暗号化によるアクセス制御を用いて対応することができる。暗号化によるアクセス制御はデータの保存者がデータを盗み見る可能性を心配する必要がないという意味において、データの保護に関して強力な方法である。本実施形態の再暗号化システムを用いることにより、アクセス権限を容易に変更することができるので、暗号化によるアクセス制御の利用対象を大きく広げることができる。

[0067] 図 5 は、本発明による再暗号化システムの主要部を示すブロック図である。図 5 に示すように、本発明による再暗号化システム 1 0 0 は、主要な構成として、管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する代理鍵生成部 2 1 5 を備えたことを特徴とする。

[0068] また、上記の各実施形態には以下の（１）～（４）に示す再暗号化システ

ムも開示されている。

[0069] (1) 管理者が保有するマスター鍵（例えば、マスター鍵 205）、変更前の復号可能者集合（例えば、復号可能者集合 203）、変更後の復号可能者集合（例えば、新しい復号可能者集合 210）とを入力し、変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文（例えば、暗号文 209）を、変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文（例えば、暗号文 222）に変換するための代理鍵（例えば、代理鍵 216）を生成して出力する代理鍵生成部（例えば、代理鍵生成部 215）を備えた再暗号化システム。

[0070] (2) 再暗号化システムは、変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文、および代理鍵を入力し、変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を生成して出力する再暗号化部（例えば、再暗号化部 221）を備えるように構成されていてもよい。

[0071] (3) 再暗号化システムは、復号者の識別子と、代理鍵の生成により得られた更新情報（例えば、更新情報 217）のうちの少なくとも一部と、識別子で特定される復号者の秘密鍵を入力し、識別子で特定される復号者の新しい秘密鍵を出力する鍵更新部（例えば、鍵更新部 219）を備え、更新情報は、公開鍵の更新に関する情報を含み、秘密鍵は、復号者の識別子を含む復号可能者集合を指定して、古い公開鍵を用いて生成された暗号文を復号可能であり、新しい秘密鍵は、復号者の識別子を含む復号可能者集合を指定して、新しい公開鍵を用いて生成された暗号文を復号可能であるように構成されていてもよい。

[0072] (4) 復号者識別子、マスター鍵、および公開鍵を入力して復号者秘密鍵を生成する鍵導出部と代理鍵を生成する代理鍵生成部とを含む管理部（例えば、管理部 301）と、データを送受信する送受信部（例えば、送受信部 321）と再暗号化部（例えば、再暗号化部 221）とを含み、データ登録者により暗号化され登録された暗号文を保存し、要求に応じて当該暗号文を送信するデータ保存部（例えば、データ保存部 302）とを備え、管理部は、代

理鍵生成部が生成した代理鍵をデータ保存部に送信し、データ保存部は、代理鍵を受け取り、保存した暗号文を再暗号化部により再暗号化し、暗号文を再暗号化された暗号文に入れ替えるように構成されていてもよい。

[0073] この出願は、2012年8月30日に提出された日本出願特願2012-189548を基礎とする優先権を主張し、その開示の全てをここに取り込む。

[0074] 以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

産業上の利用の可能性

[0075] 本発明は、クラウド等を利用したデータ保存サービスに適用できる。

符号の説明

- [0076] 206 暗号化部
207 鍵導出部
213 復号部
215 代理鍵生成部
219 鍵更新部
220 設定部
221 再暗号化部
301 管理部
302 データ保存部
303 データ登録部
304 データ復号部
321 送受信部
322 暗号文記憶部

請求の範囲

- [請求項1] 管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する代理鍵生成部を備えたことを特徴とする再暗号化システム。
- [請求項2] 前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文、および代理鍵を入力し、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を生成して出力する再暗号化部を備えた請求項1記載の再暗号化システム。
- [請求項3] 復号者の識別子と、代理鍵の生成により得られた更新情報のうちの少なくとも一部と、前記識別子で特定される復号者の秘密鍵を入力し、前記識別子で特定される復号者の新しい秘密鍵を出力する鍵更新部を備え、
前記更新情報は、公開鍵の更新に関する情報を含み、
前記秘密鍵は、前記復号者の識別子を含む復号可能者集合を指定して、古い公開鍵を用いて生成された暗号文を復号可能であり、
前記新しい秘密鍵は、前記復号者の識別子を含む復号可能者集合を指定して、新しい公開鍵を用いて生成された暗号文を復号可能である請求項1または請求項2記載の再暗号化システム。
- [請求項4] 復号者識別子、マスター鍵、および公開鍵を入力して復号者秘密鍵を生成する鍵導出部と代理鍵を生成する代理鍵生成部とを含む管理部と、
データを送受信する送受信部と再暗号化部とを含み、データ登録者により暗号化され登録された暗号文を保存し、要求に応じて当該暗号文を送信するデータ保存部とを備え、

前記管理部は、

前記代理鍵生成部が生成した代理鍵を前記データ保存部に送信し、

前記データ保存部は、

前記代理鍵を受け取り、保存した前記暗号文を前記再暗号化部により再暗号化し、前記暗号文を再暗号化された暗号文に入れ替える

請求項 2 記載の再暗号化システム。

[請求項5]

管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する

ことを特徴とする再暗号化方法。

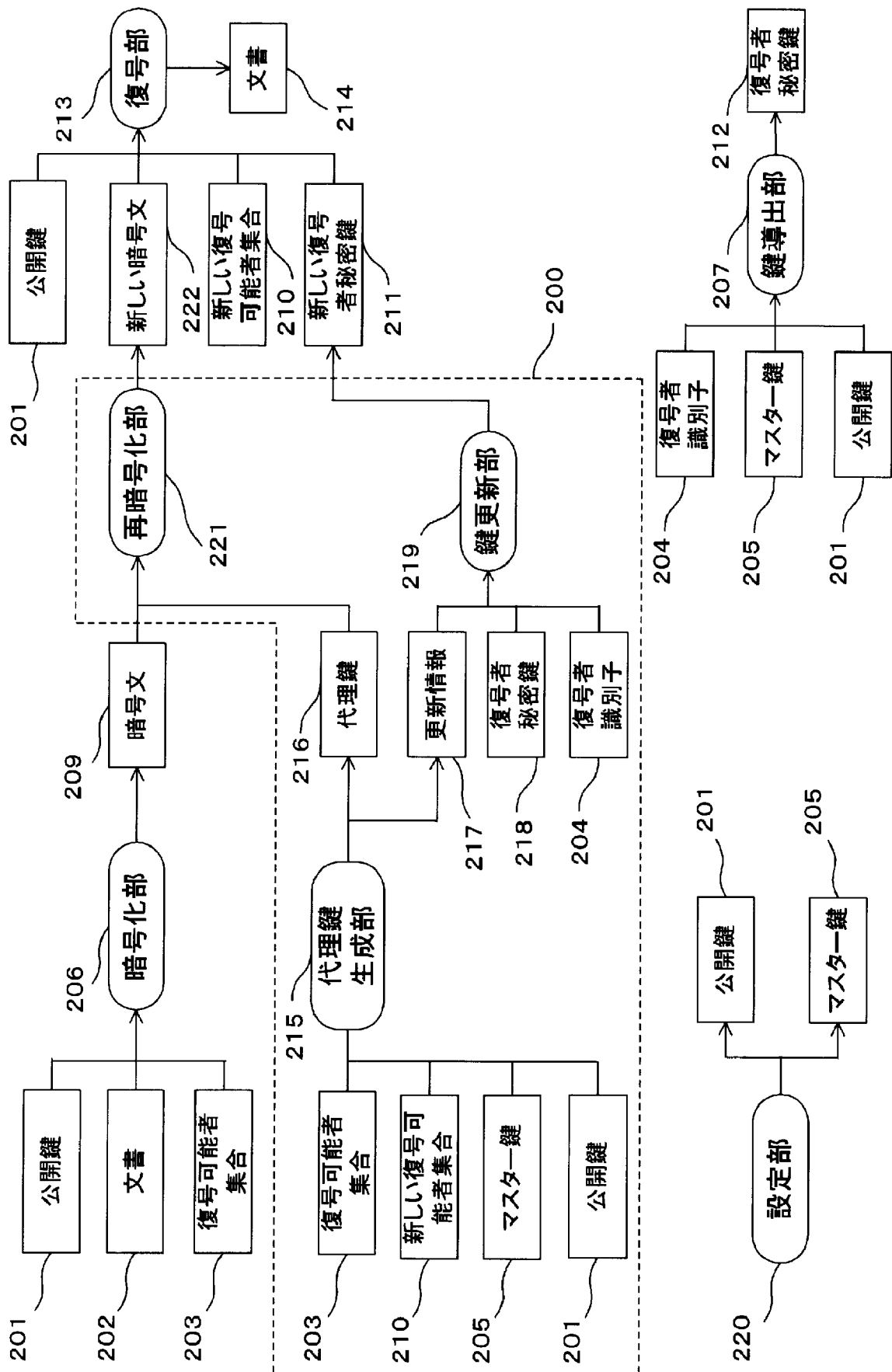
[請求項6]

コンピュータに、

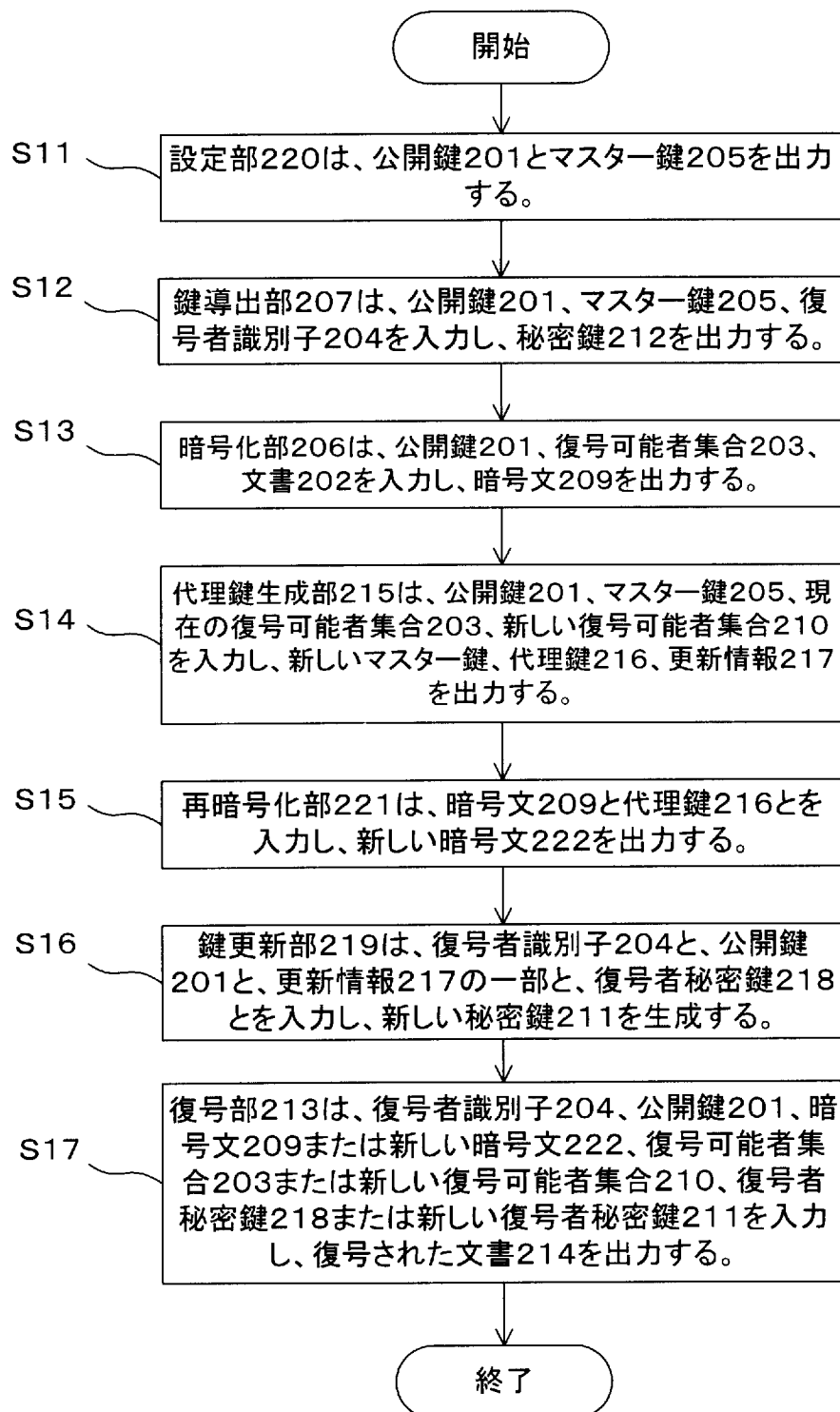
管理者が保有するマスター鍵、変更前の復号可能者集合、変更後の復号可能者集合とを入力し、前記変更前の復号可能者集合に属する復号者の秘密鍵で復号可能な暗号文を、前記変更後の復号可能者集合に属する復号者の秘密鍵で復号可能な新しい暗号文に変換するための代理鍵を生成して出力する代理鍵生成処理

を実行させるための再暗号化プログラム。

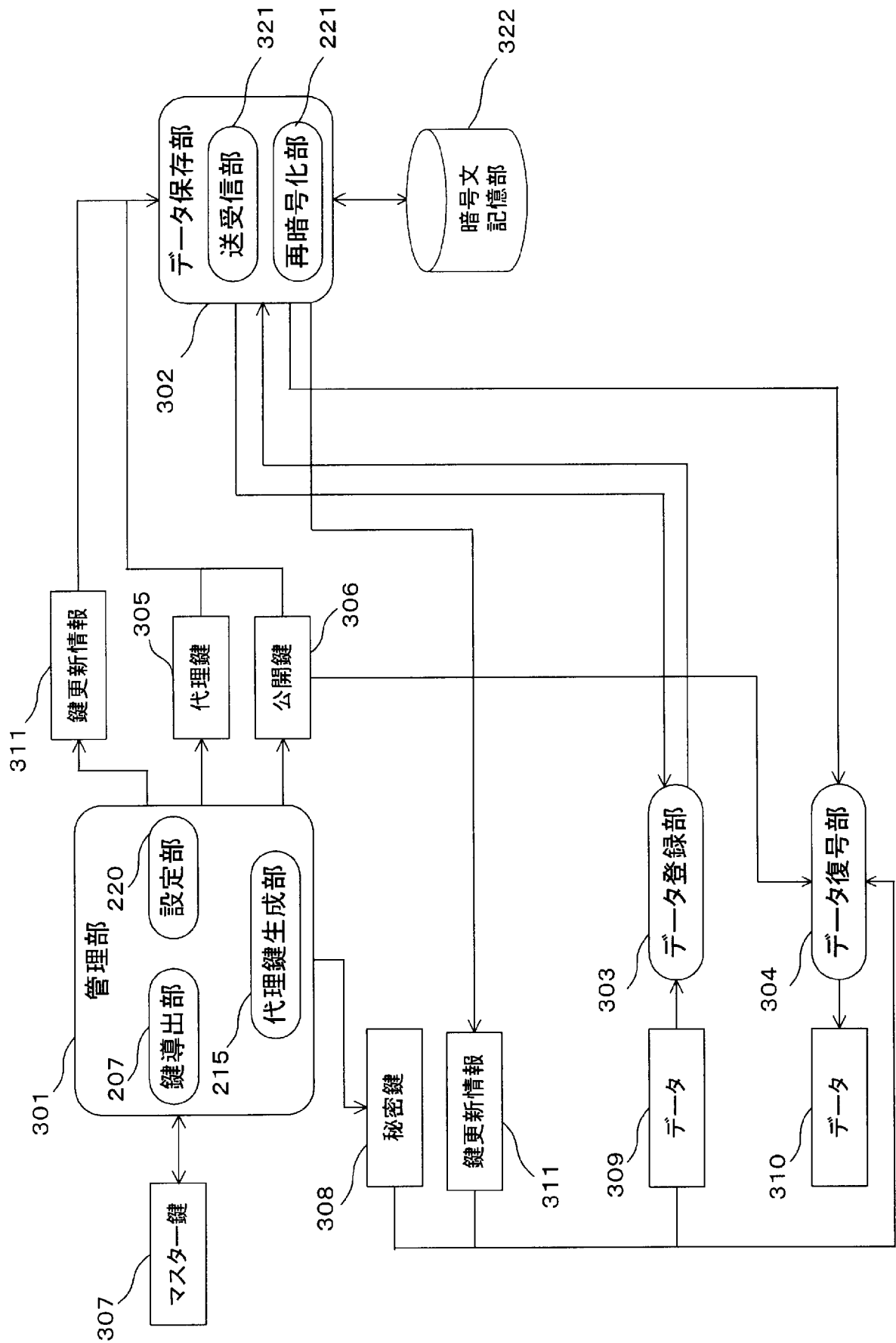
[図1]



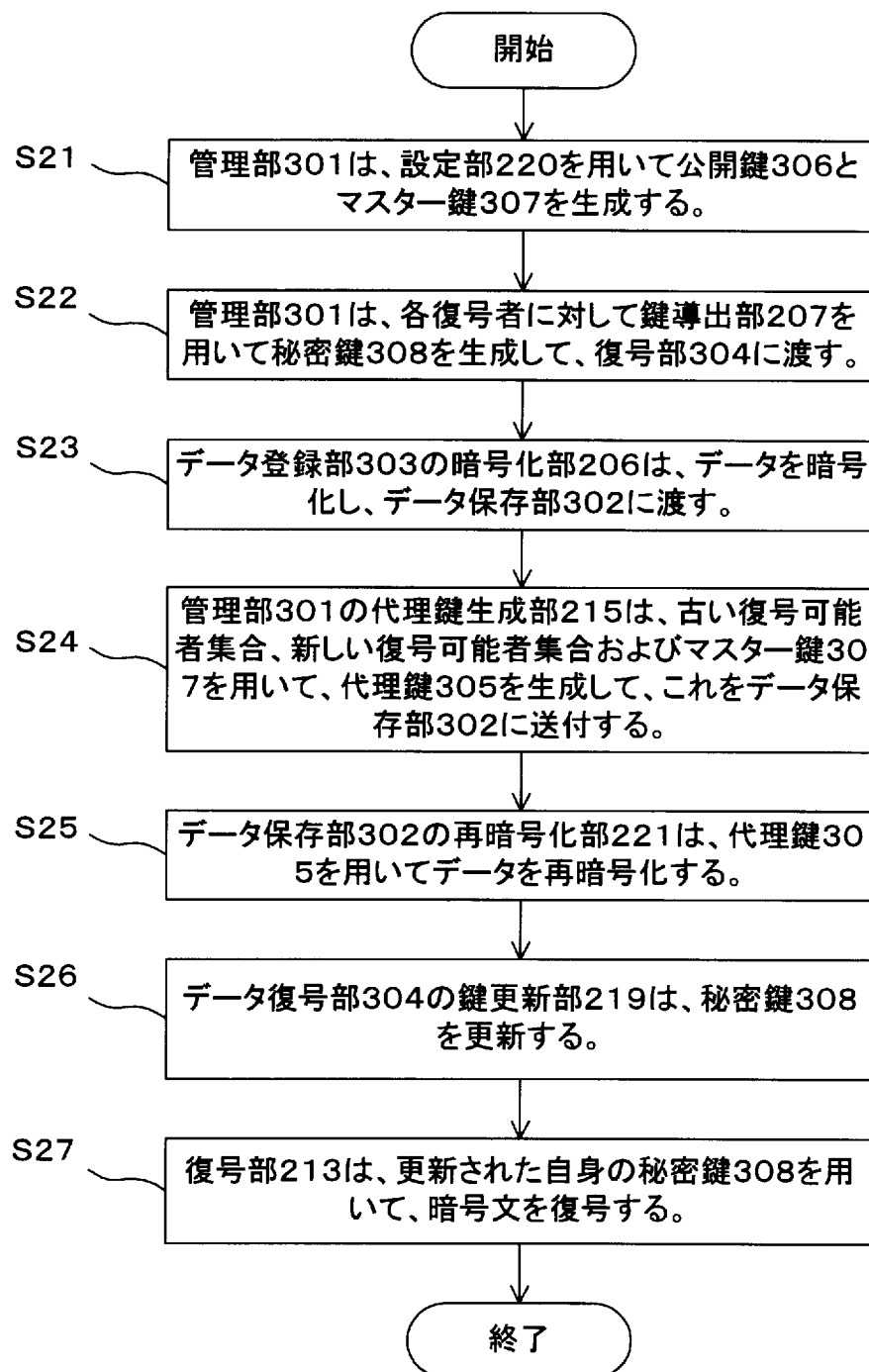
[図2]



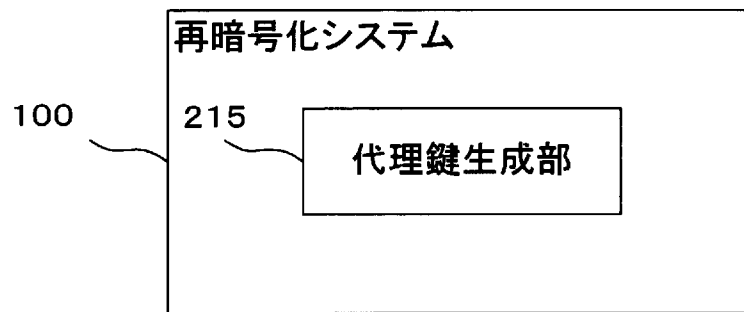
[図3]



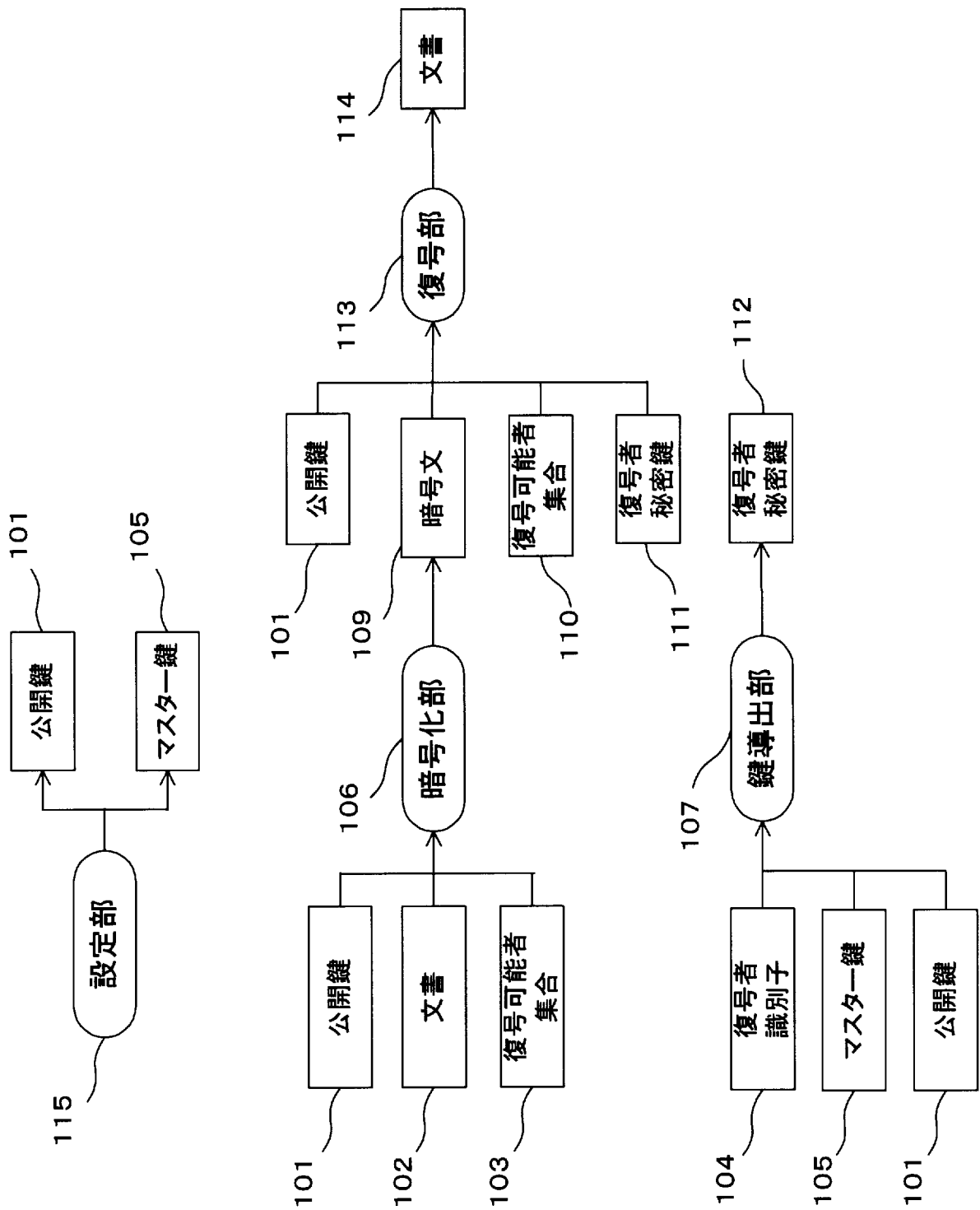
[図4]



[図5]



[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2013/004576

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01) i, G06F21/62(2013.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/08, G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2012-150378 A (Nippon Telegraph and Telephone Corp.), 09 August 2012 (09.08.2012), paragraphs [0016] to [0027] (Family: none)	1, 2, 5, 6 3, 4
Y A	JP 2000-244474 A (Nippon Telegraph and Telephone Corp.), 08 September 2000 (08.09.2000), paragraphs [0091] to [0096] (Family: none)	1, 2, 5, 6 3, 4
A	Cheng-Kang CHU et al., "Conditional Proxy Broadcast Re-Encryption", Lecture Notes in Computer Science, 2009, Vol. 5594, pp. 327-342.	1-6

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
09 August, 2013 (09.08.13)

Date of mailing of the international search report
20 August, 2013 (20.08.13)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2013/004576

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Jin SUN et al., "CCA-secure Unidirectional Proxy Broadcast Re-encryption in the Standard Model", [online], Journal of Computational Information Systems, 2012.07.15, Vol. 8, No. 14, pp. 5909-5916. [retrieved on 2013.08.08]. Retrieved from the Internet: <URL: http://www.jofcis.com/publishedpapers/2012_8_14_5909_5916.pdf >	1-6

A. 発明の属する分野の分類（国際特許分類（I P C））
Int.Cl. H04L9/08(2006.01)i, G06F21/62(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. H04L9/08, G06F21/62

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 3 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 3 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 3 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2012-150378 A（日本電信電話株式会社）2012. 08. 09, 段落 0016-0027	1, 2, 5, 6
A	（ファミリーなし）	3, 4
Y	JP 2000-244474 A（日本電信電話株式会社）2000. 09. 08, 段落 0091-0096	1, 2, 5, 6
A	（ファミリーなし）	3, 4

☒ C 欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

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

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

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

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

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

「&」同一パテントファミリー文献

国際調査を完了した日

0 9 . 0 8 . 2 0 1 3

国際調査報告の発送日

2 0 . 0 8 . 2 0 1 3

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

金沢 史明

5 S

4 5 3 8

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	Cheng-Kang CHU et al., "Conditional Proxy Broadcast Re-Encryption", Lecture Notes in Computer Science, 2009, Vol. 5594, pp. 327-342.	1-6
A	Jin SUN et al., "CCA-secure Unidirectional Proxy Broadcast Re-encryption in the Standard Model", [online], Journal of Computational Information Systems, 2012.07.15, Vol. 8, No. 14, pp. 5909-5916. [retrieved on 2013.08.08]. Retrieved from the Internet: <URL: http://www.jofcis.com/publishedpapers/2012_8_14_5909_5916.pdf >	1-6