(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
2024年10月3日(03.10.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/201635 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2023/012095

(22) 国際出願日： 2023年3月27日(27.03.2023)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人:三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

(72) 発明者:廣政 良(**HIROMASA, Ryo**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人:弁理士法人クロスボーダー特許事務所(**CROSS-BORDER PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

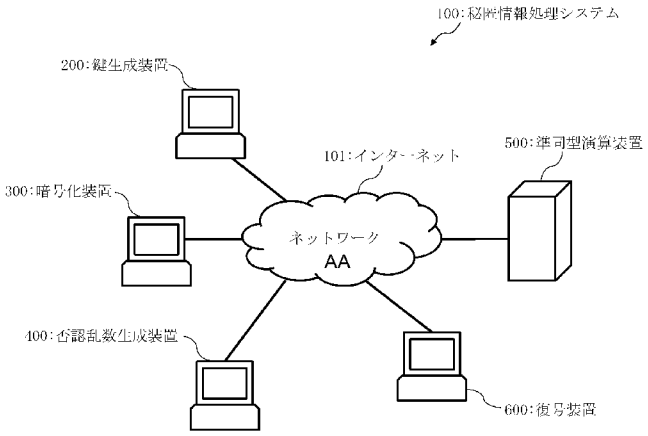
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG,

(54) **Title:** CONFIDENTIAL INFORMATION PROCESSING SYSTEM, CONFIDENTIAL INFORMATION PROCESSING METHOD, AND CONFIDENTIAL INFORMATION PROCESSING PROGRAM

(54) 発明の名称： 秘匿情報処理システム、秘匿情報処理方法、および秘匿情報処理プログラム

[図1]



100 Confidential information processing system
101 Internet
200 Key generation device
300 Encryption device
400 Denial random number generation device
500 Homomorphic computation device
600 Decryption device
AA Network

(57) **Abstract:** A key generation device (200) generates an encryption key PK, a decryption key SK, and a homomorphic computation key EVK. An encryption device (300) generates encrypted data C_{DPK} (m) obtained by encrypting plaintext data m with the encryption key PK. A denial random number generation device (400) uses the encryption key PK and the encrypted text data C_{DPK} (m) as inputs, and generates denial random number data r^* for denying the disclosure of the plain text data m. A homomorphic computation device (500) generates post-homomorphic-computation encrypted text data C_{MPK} (M) obtained by performing homomorphic computation on the calculation result of the plain text data with the homomorphic computation key EVK. A decryption device (600) decodes the post-homomorphic-computation encrypted text data C_{MPK} (M).

WO 2024/201635 A1

[続葉有]

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, ME, 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：

一　国際調査報告（条約第21条(3)）

(57) 要約：鍵生成装置（２００）は、暗号化鍵ＰＫと復号鍵ＳＫと準同型演算鍵ＥＶＫを生成する。暗号化装置（３００）は、暗号化鍵ＰＫで平文データｍを暗号化した暗号化データC_{DPK}（ｍ）を生成する。否認乱数生成装置（４００）は、暗号化鍵ＰＫと暗号文データC_{DPK}（ｍ）とを入力とし、平文データｍの開示の否認のための否認乱数データr^{*}を生成する。準同型演算装置（５００）は、準同型演算鍵ＥＶＫで平文データの計算結果を準同型演算した準同型演算後暗号文データC_{MPK}（Ｍ）を生成する。復号装置（６００）は、準同型演算後暗号文データC_{MPK}（Ｍ）を復号する。

明　細　書

発明の名称 ：

秘匿情報処理システム、秘匿情報処理方法、および秘匿情報処理プログラム

技術分野

[0001] 本開示は、秘匿情報処理システム、秘匿情報処理方法、および秘匿情報処理プログラムに関する。

背景技術

[0002] 準同型暗号とは、データを暗号化したまま分析処理できる暗号技術である。昨今、クラウドサービスの利用が広まりつつあるが、クラッキングあるいはクラウドの信頼性の懸念から、クラウド上ではデータを暗号化して保管することが考えられる。準同型暗号は、暗号化されているデータに対して、復号することなく演算を施すことができるため、安全性を損なうことなくクラウドサービスの利用を可能とする技術である。

[0003] 準同型暗号の安全性を向上するために、暗号文に暗号化されているデータに対して、例えば政府といった特権的なユーザによる強制的なデータ開示を防ぐための機能が否認可能性である。

一般的な公開鍵暗号技術における暗号化アルゴリズムは、平文データを暗号化するために公開鍵データと乱数データを用いる。公開鍵データは公開情報なので、平文データと乱数データが決まれば暗号文データは一意に定まる。否認可能性は、ある暗号文データに実際に暗号化されている平文データとは異なるデータをその暗号文データに暗号化するための乱数データを生成することができる性質である。この性質により、クラウドサービスに分析処理を委託するためにユーザが保存している暗号文データに対して、ユーザは偽のデータをその暗号文データに暗号化できる乱数データを生成することできる。これにより、特権的なユーザから平文データの開示を強制されたときに、データの強制開示から逃れることができる。

[0004] 非特許文献１には、否認可能性を満たす準同型暗号の初めての構成例が記されている。

先行技術文献

非特許文献

[0005] 非特許文献1：Ｓｈｗｅｔａ Ａｇｒａｗａｌ，Ｓｈａｆｉ Ｇｏｌｄｗａｓｓｅｒ，ａｎｄ Ｓａｌｅｅｔ Ｍｏｓｓｅｌ．Ｄｅｎｉａｂｌｅ Ｆｕｌｌｙ Ｈｏｍｏｍｏｒｐｈｉｃ Ｅｎｃｒｙｐｔｉｏｎ ｆｒｏｍ ＬＷＥ．Ｉｎ ＣＲＹＰＴＯ，ｐａｇｅｓ ６４１－６７０，２０２１．

非特許文献2：Ａｄｒｉａｎａ Ｌｏｐｅｚ－Ａｌｔ，Ｅｒａｎ Ｔｒｏｍｅｒ，ａｎｄ Ｖｉｎｏｄ Ｖａｉｋｕｎｔａｎａｔｈａｎ．Ｏｎ－ｔｈｅ－Ｆｌｙ Ｍｕｌｔｉｐａｒｔｙ Ｃｏｍｐｕｔａｔｉｏｎ ｏｎ ｔｈｅ Ｃｌｏｕｄ ｖｉａ Ｍｕｌｔｉｋｅｙ Ｆｕｌｌｙ Ｈｏｍｏｍｏｒｐｈｉｃ Ｅｎｃｒｙｐｔｉｏｎ．Ｉｎ ＳＴＯＣ，ｐａｇｅｓ １２１９－１２３４，２０１２．

発明の概要

発明が解決しようとする課題

[0006] 非特許文献１で示されている否認可能性を持つ準同型暗号は、同じ鍵の下で暗号化された暗号文データ同士でしか分析処理できない。そのため、非特許文献１で示されている否認可能準同型暗号を用いたクラウドサービスで様々なユーザのデータを用いて分析処理を行う場合、ユーザ同士で鍵を共有する必要があり、ユーザ間でのデータの秘匿性が担保されない。

[0007] 本開示では、各々のユーザが異なる鍵を用いてデータを暗号化できるような否認可能準同型暗号を実現することを目的とする。

課題を解決するための手段

[0008] 本開示に係る秘匿情報処理システムは、

暗号化鍵ＰＫと復号鍵ＳＫと準同型演算鍵ＥＶＫを生成する鍵生成装置と

、

前記暗号化鍵ＰＫで平文データｍを暗号化した暗号化データC_{DPK}（ｍ）を生成する暗号化装置と、

前記暗号化鍵ＰＫと暗号文データC_{DPK}（ｍ）とを入力とし、平文データｍの開示の否認のための否認乱数データｒ*を生成する否認乱数生成装置と、

前記準同型演算鍵ＥＶＫで平文データの計算結果を準同型演算した準同型演算後暗号文データC_{MPK}（Ｍ）を生成する準同型演算装置と、

準同型演算後暗号文データを復号する復号装置とを備える。

発明の効果

[0009] 本開示に係る秘匿情報処理システムでは、継続的な秘匿情報処理を、対象者にとって無意識的に実現することにより、対象者の入れ替わりあるいはなりすましの検出を行うことができる。

図面の簡単な説明

[0010] [図1]実施の形態１に係る秘匿情報処理システムのシステム構成例を示す図。

[図2]実施の形態１に係る鍵生成装置の構成を示すブロック図。

[図3]実施の形態１に係る暗号化装置の構成を示すブロック図。

[図4]実施の形態１に係る否認乱数生成装置の構成を示すブロック図。

[図5]実施の形態１に係る準同型演算装置の構成を示すブロック図。

[図6]実施の形態１に係る復号装置の構成を示すブロック図。

[図7]実施の形態１に係る秘匿情報処理システムの各装置の動作を示すフローチャート。

[図8]実施の形態１に係る秘匿情報処理システムの準同型演算を示すフローチャート。

[図9]実施の形態１に係る秘匿情報処理システムの準同型演算を示すフローチャート。

[図10]実施の形態１に係る秘匿情報処理システムの各装置のハードウェア構成例を示す図。

[図11]実施の形態１の変形例に係る秘匿情報処理システムの各装置のハード

ウェア構成例を示す図。

発明を実施するための形態

[0011] 以下、本実施の形態について、図を用いて説明する。各図中、同一または相当する部分には、同一符号を付している。実施の形態の説明において、同一または相当する部分については、説明を適宜省略または簡略化する。図中の矢印はデータの流れまたは処理の流れを主に示している。

[0012] 実施の形態１．

＊＊＊構成の説明＊＊＊

図１は、本実施の形態に係る秘匿情報処理システム１００のシステム構成例を示す図である。

秘匿情報処理システム１００は、鍵生成装置２００と、暗号化装置３００と、否認乱数生成装置４００と、準同型演算装置５００と、復号装置６００とを有する。

インターネット１０１は、鍵生成装置２００と、複数の暗号化装置３００と、否認乱数生成装置４００と、準同型演算装置５００と、復号装置６００とを接続する通信路である。インターネット１０１は、ネットワークの例である。インターネット１０１の代わりに、他の種類のネットワークが用いられてもよい。

[0013] 鍵生成装置２００は、例えば、ＰＣである。ＰＣは、Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒの略語である。

鍵生成装置２００は、暗号化に利用する暗号化鍵と、準同型演算に利用する準同型演算鍵と、暗号文データの復号に利用する復号鍵を作成する。鍵生成装置２００は、インターネット１０１を介して、暗号化装置３００と否認乱数生成装置４００へ暗号化鍵を、準同型演算装置５００へ準同型演算鍵を送信し、復号装置６００へ復号鍵を送信する。なお、これらの鍵は、郵送などで直接的に送信してもよい。復号鍵は秘密の情報であるため、漏えいしないよう鍵生成装置２００と復号装置６００の内部に保管される。

[0014] 暗号化装置３００は、暗号化鍵で平文データを暗号化した暗号化データを

生成する。暗号化装置３００は、単一の暗号化鍵を用いて平文データを暗号化した暗号化データを生成する。暗号化装置３００は、例えば、ＰＣである。暗号化装置３００は、工場のセンサなどから得られた平文データを、保管している暗号化鍵で暗号化することで暗号文データを生成する。暗号化装置３００は、暗号文データを準同型演算装置５００に送信する。

[0015] 否認乱数生成装置４００は、暗号化鍵と暗号文データとを入力とし、平文データの開示の否認のための否認乱数データを生成する。否認乱数生成装置４００は、例えば、ＰＣである。否認乱数生成装置４００は、鍵生成装置２００から送られてきた暗号化鍵を受信し、暗号化鍵を保管する暗号化鍵保管装置としても機能する。

否認乱数生成装置４００は、暗号化装置３００から送られてきた、暗号文データと、平文データと、乱数データから、否認乱数データを生成し、保管する。

[0016] 準同型演算装置５００は、準同型演算鍵と暗号化データとを入力とし、平文データの計算結果を準同型演算した準同型演算後暗号文データを生成する。準同型演算装置５００は、例えば、大容量の記憶媒体を持つ計算機である。準同型演算装置５００は、データ保管装置としても機能する。すなわち、準同型演算装置５００は、暗号化装置３００から暗号文データの保管要求があればそれらの暗号文データを保管する。

準同型演算装置５００は、保管暗号文データに対して準同型演算を行う装置としても機能する。すなわち、準同型演算装置５００は、保管準同型演算鍵と、保管暗号文データから、暗号文データの平文データに対する演算結果の暗号文データ（準同型演算後暗号文データ）を生成し、復号装置６００に送信する。保管準同型演算鍵は準同型演算装置５００に保管されている準同型演算鍵である。保管暗号文データは準同型演算装置５００に保管されている暗号文データである。

[0017] 復号装置６００は、準同型演算後暗号文データを復号する。復号装置６００は、例えば、ＰＣである。復号装置６００は、鍵生成装置２００から送ら

れてきた復号鍵を受信し、復号鍵を保管する復号鍵保管装置としても機能する。

復号装置６００は、準同型演算装置５００から送られてきた、暗号文データ（準同型演算後暗号文データ）を受け取り、保管されている復号鍵で復号することで演算結果を取得する暗号文データ復号装置として動作するＰＣでもある。

[0018] なお、同じＰＣ内に、鍵生成装置２００、暗号化装置３００、否認乱数生成装置４００、準同型演算装置５００、および復号装置６００のいずれかが同時に含まれていてもよい。

[0019] 以下、本実施の形態の構成について説明する。

図１に示したように、秘匿情報処理システム１００は、鍵生成装置２００と、暗号化装置３００と、否認乱数生成装置４００と、準同型演算装置５００と、復号装置６００とを備える。以下では、鍵生成装置２００の構成、暗号化装置３００の構成、否認乱数生成装置４００の構成、準同型演算装置５００の構成、復号装置６００の構成について順番に説明する。

[0020] 図２は、本実施の形態に係る鍵生成装置２００の構成を示すブロック図である。

図２に示すように、鍵生成装置２００は、機能要素として、入力部２０１と、否認可能復号鍵生成部２０２と、否認可能暗号化鍵生成部２０３と、複数鍵準同型復号鍵生成部２０４と、複数鍵準同型暗号化鍵生成部２０５と、準同型演算鍵生成部２０６と、送信部２０７とを備える。

また、図示していないが、鍵生成装置２００は、鍵生成装置２００の各部で使用されるデータを記憶する記憶部を備える。

[0021] 入力部２０１は、セキュリティパラメータλを受け取り、セキュリティパラメータλを否認可能復号鍵生成部２０２と複数鍵準同型復号鍵生成部２０４へ送る。

否認可能復号鍵生成部２０２は、入力部２０１から受け取ったセキュリティパラメータλを入力として、否認可能復号鍵ＤＳＫを生成する。さらに、

否認可能復号鍵生成部２０２は、否認可能復号鍵ＤＳＫを否認可能暗号化鍵生成部２０３と準同型演算鍵生成部２０６と送信部２０７へ送る。

否認可能暗号化鍵生成部２０３は、否認可能復号鍵生成部２０２から受け取った否認可能復号鍵ＤＳＫを入力として、否認可能暗号化鍵ＤＰＫを生成する。さらに、否認可能暗号化鍵生成部２０３は、否認可能暗号化鍵ＤＰＫを送信部２０７へ送る。

[0022] 複数鍵準同型復号鍵生成部２０４は、入力部２０１から受け取ったセキュリティパラメータλを入力として、複数鍵準同型復号鍵ＭＳＫを生成する。さらに、複数鍵準同型復号鍵生成部２０４は、複数鍵準同型復号鍵ＭＳＫを複数鍵準同型暗号化鍵生成部２０５と送信部２０７へ送る。

複数鍵準同型暗号化鍵生成部２０５は、複数鍵準同型復号鍵生成部２０４から受け取った複数鍵準同型復号鍵ＭＳＫを入力として、複数鍵準同型暗号化鍵ＭＰＫを生成する。さらに、複数鍵準同型暗号化鍵生成部２０５は、複数鍵準同型暗号化鍵ＭＰＫを準同型演算鍵生成部２０６と送信部２０７へ送る。

[0023] 準同型演算鍵生成部２０６は、否認可能復号鍵生成部２０２から受け取った否認可能復号鍵ＤＳＫと、複数鍵準同型暗号化鍵生成部２０５から受け取った複数鍵準同型暗号化鍵ＭＰＫを入力として、準同型演算鍵ＥＶＫを生成する。さらに、準同型演算鍵生成部２０６は、準同型演算鍵ＥＶＫを送信部２０７へ送る。

[0024] 送信部２０７は、否認可能復号鍵生成部２０２で生成された否認可能復号鍵ＤＳＫと複数鍵準同型復号鍵生成部２０４で生成された複数鍵準同型復号鍵ＭＳＫから復号鍵ＳＫ＝（ＤＳＫ，ＭＳＫ）を生成し、復号装置６００へ送信する。または、否認可能暗号化鍵生成部２０３で生成された否認可能暗号化鍵ＤＰＫと複数鍵準同型暗号化鍵生成部２０５で生成された複数鍵準同型暗号化鍵ＭＰＫから暗号化鍵ＰＫを生成し、暗号化装置３００と否認乱数生成装置４００へ送信する。または、準同型演算鍵生成部２０６で生成された準同型演算鍵ＥＶＫを準同型演算装置５００へ送信する。

[0025] 図３は、本実施の形態に係る暗号化装置３００の構成を示すブロック図である。

図３に示すように、暗号化装置３００は、機能要素として、入力部３０１と、暗号化鍵保管部３０２と、平文保管部３０３と、乱数生成部３０４と、暗号化部３０５と、乱数保管部３０６と、送信部３０７とを備える。

また、図示していないが、暗号化装置３００は、暗号化装置３００の各部で使用されるデータを記憶する記憶部を備える。

[0026] 入力部３０１は、鍵生成装置２００から送信されてきた暗号化鍵ＰＫを受け取り、暗号化鍵保管部３０２へ送信する。または、入力部３０１は、平文データｍを受け取り、それらの平文データｍを平文保管部３０３へ送信する。

暗号化鍵保管部３０２は、入力部３０１から受け取った暗号化鍵ＰＫを保管する。

平文保管部３０３は、入力部３０１から受け取った平文データｍを保管する。

乱数生成部３０４は、暗号化鍵保管部３０２に保存されている暗号化鍵ＰＫから乱数データｒを生成し暗号化部３０５と乱数保管部３０６へ送信する。

[0027] 暗号化部３０５は、暗号化鍵保管部３０２から送信された暗号化鍵ＰＫと、平文保管部３０３から送信された平文データｍと、乱数生成部３０４から乱数データｒを受け取り、平文データｍの暗号文データC_{PK}（ｍ）を生成する。そして、暗号化部３０５は、暗号文データC_{PK}（ｍ）を送信部３０７へ送信する。以降では、C_{PK}（ｍ）で平文データｍを暗号化鍵ＰＫで暗号化して得られる暗号文データを表す。

乱数保管部３０６は、乱数生成部３０４から受け取った乱数データｒを保管する。

送信部３０７は、暗号化部３０５から暗号文データC_{PK}（ｍ）を受け取り、否認乱数生成装置４００と準同型演算装置５００へ送信する。

[0028] 図４は、本実施の形態に係る否認乱数生成装置４００の構成を示すブロック図である。

図４に示すように、否認乱数生成装置４００は、機能要素として、入力部４０１と、暗号化鍵保管部４０２と、否認乱数生成部４０３と、否認乱数保管部４０４とを備える。

また、図示していないが、否認乱数生成装置４００は、否認乱数生成装置４００の各部で使用されるデータを記憶する記憶部を備える。

[0029] 入力部４０１は、鍵生成装置２００から送信されてきた暗号化鍵ＰＫを受信し、暗号化鍵保管部４０２へ送る。または、暗号化装置３００から送信されてきた暗号文データC_{PK}（ｍ）と乱数データｒを受信し、否認乱数生成部４０３へ送る。

暗号化鍵保管部４０２は、否認乱数生成装置４００の入力部４０１から受け取った暗号化鍵ＰＫを保管する。

否認乱数生成部４０３は、入力部４０１から受け取った暗号文データC_{PK}（ｍ）と乱数データｒと、暗号化鍵保管部４０２に保管されている暗号化鍵ＰＫから、否認乱数データｒ*を生成し、否認乱数保管部４０４へ送る。

否認乱数保管部４０４は、否認乱数生成部４０３から受け取った否認乱数データｒ*を保管する。

[0030] 図５は、本実施の形態に係る準同型演算装置５００の構成を示すブロック図である。

図５に示すように、準同型演算装置５００は、機能要素として、入力部５０１と、準同型演算鍵保管部５０２と、暗号文保管部５０３と、演算処理構成部５０４と、準同型演算部５０５と、送信部５０６とを備える。

また、図示していないが、準同型演算装置５００は、準同型演算装置５００の各部で使用されるデータを記憶する記憶部を備える。

[0031] 入力部５０１は、鍵生成装置２００から送信されてきた準同型演算鍵ＥＶＫ１とＥＶＫ２を受信し、準同型演算鍵保管部５０２へ送る。または、暗号化装置３００から送信されてきた暗号文データC_{PK1}（ｍ１）とC_{PK2}（ｍ２

）を受信し、暗号文保管部５０３へ送る。または、演算回路ｆを受信し、演算処理構成部５０４へ送る。

[0032] 準同型演算鍵保管部５０２は、入力部５０１から受け取った準同型演算鍵ＥＶＫ１とＥＶＫ２を保管する。

暗号文保管部５０３は、入力部５０１から受け取った暗号文データC_{PK1}（ｍ１）と暗号文データC_{PK2}（ｍ２）を保管する。

演算処理構成部５０４は、入力部５０１から受け取った演算回路ｆと、暗号文保管部５０３から受け取った暗号文データC_{PK1}（ｍ１）とC_{PK2}（ｍ２）を入力として、準同型演算回路Ｃを生成する。

[0033] 準同型演算部５０５は、準同型演算鍵保管部５０２から準同型演算鍵ＥＶＫ１とＥＶＫ２と、演算処理構成部５０４から準同型演算回路Ｃとを受けとり、平文データｍ１と平文データｍ２に演算回路ｆを適用して得られる演算結果データＭ＝ｆ（ｍ１，ｍ２）に関する暗号文データC_{PK}（Ｍ）を計算し、送信部５０６へ送る。ここで、ｆ（ｍ１，ｍ２）は、２つの平文データｍ１、ｍ２を入力として演算回路ｆを計算した結果を表し、ＰＫは暗号化鍵ＰＫ１とＰＫ２からなる集合｛ＰＫ１、ＰＫ２｝を表す。また、以降ではC_{PK}（Ｍ）で、暗号化鍵集合ＰＫ＝｛ＰＫ１、ＰＫ２｝に関する演算結果データＭの準同型演算後暗号文データを表す。準同型演算後暗号文データC_{PK}（Ｍ）からは、復号鍵ＳＫ１とＳＫ２を用いることで、演算結果データＭを復号できる。

送信部５０６は、準同型演算部５０５から受け取った準同型演算後暗号文データC_{PK}（Ｍ）を復号装置６００に送信する。

[0034] 図６は、本実施の形態に係る復号装置６００の構成を示すブロック図である。

図６に示すように、復号装置６００は、機能要素として、入力部６０１と、復号鍵保管部６０２と、復号処理部６０３と、復号結果保管部６０４とを備える。

また、図示していないが、復号装置６００は、復号装置６００の各部で使

用されるデータを記憶する記憶部を備える。

[0035] 入力部６０１は、鍵生成装置２００から送信された復号鍵ＳＫ１とＳＫ２とを受信する。または、準同型演算装置５００から送信された暗号化鍵の集合ＰＫ＝｛ＰＫ１，ＰＫ２｝に関する演算結果データＭの準同型演算後暗号文データC_{PK}（Ｍ）を受信する。

復号鍵保管部６０２は、入力部６０１から受け取った復号鍵ＳＫ１とＳＫ２とを保管する。

復号処理部６０３は、入力部６０１から準同型演算後暗号文データC_{PK}（Ｍ）と、復号鍵保管部６０２から復号鍵ＳＫ１とＳＫ２とを受け取る。復号処理部６０３は、準同型演算後暗号文データC_{PK}（Ｍ）を復号鍵ＳＫ１とＳＫ２とで、暗号化されていた演算結果データＭを復号し、復号結果保管部６０４へ送る。

復号結果保管部６０４は、復号処理部６０３から演算結果データＭを受け取り、保管する。

[0036] ＊＊＊動作の説明＊＊＊

次に、本実施の形態に係る秘匿情報処理システム１００の動作について説明する。秘匿情報処理システム１００の動作手順は、秘匿情報処理方法に相当する。また、秘匿情報処理システム１００の動作を実現するプログラムは、秘匿情報処理プログラムに相当する。

[0037] 図７は、本実施の形態に係る秘匿情報処理システム１００の各装置の動作を示すフローチャートである。

図７のフローチャートでは、暗号化鍵・復号鍵・準同型演算鍵の生成・保管処理を示している。

[0038] 図７のステップＳ７０１からステップＳ７１３は、鍵生成装置２００と、暗号化装置３００と、否認乱数生成装置４００、準同型演算装置５００と、復号装置６００とが実行する処理である。

ステップＳ７０１からステップＳ７０５は、鍵生成装置２００によって実行される。

ステップＳ７０６からステップＳ７０７は、暗号化装置３００によって実行される。

ステップＳ７０８からステップＳ７０９は、否認乱数生成装置４００によって実行される。

ステップＳ７１０からステップＳ７１１は、準同型演算装置５００によって実行される。

ステップＳ７１２からステップＳ７１３は、復号装置６００によって実行される。

[0039] ステップＳ７０１において、鍵生成装置２００の入力部２０１は、セキュリティパラメータλを受信する。

ステップＳ７０２において、鍵生成装置２００の否認可能復号鍵生成部２０２は、ステップＳ７０１において鍵生成装置２００の入力部２０１が受信したセキュリティパラメータλを入力として、否認可能復号鍵ＤＳＫを生成する。さらに、鍵生成装置２００の複数鍵準同型復号鍵生成部２０４は、ステップＳ７０１において鍵生成装置２００の入力部２０１が受信したセキュリティパラメータλを入力として、複数鍵準同型復号鍵ＭＳＫを生成する。ここで、否認可能復号鍵ＤＳＫは、非特許文献１記載の鍵生成アルゴリズムを用いて生成される。また、複数鍵準同型復号鍵ＭＳＫは非特許文献２記載の鍵生成アルゴリズムを用いて生成される。

[0040] ステップＳ７０３において、鍵生成装置２００の否認可能暗号化鍵生成部２０３は、否認可能復号鍵ＤＳＫを入力として、否認可能暗号化鍵ＤＰＫを生成する。さらに、鍵生成装置２００の複数鍵準同型暗号化鍵生成部２０５は、複数鍵準同型復号鍵ＭＳＫを入力として、複数鍵準同型暗号化鍵ＭＰＫを生成する。ここで、否認可能暗号化鍵ＤＰＫは非特許文献１記載の鍵生成アルゴリズムを用いて生成される。また、複数鍵準同型暗号化鍵ＭＰＫは非特許文献２記載の鍵生成アルゴリズムを用いて生成される。

[0041] ステップＳ７０４において、鍵生成装置２００の準同型演算鍵生成部２０６は、準同型演算鍵ＥＶＫとして、否認可能復号鍵ＤＳＫを複数鍵準同型暗

号で暗号化した複数鍵準同型暗号文を出力する。具体的には、準同型演算鍵生成部２０６は、否認可能復号鍵ＤＳＫと、複数鍵準同型暗号化鍵ＭＰＫとを入力として、以下の（数１）の形式で準同型演算鍵ＥＶＫを生成する。

[0042] ＥＶＫ＝Ｅｎｃ（ＭＰＫ，ＤＳＫ）　（数１）

ここで、アルゴリズムＥｎｃは非特許文献２記載の暗号化アルゴリズムである。

[0043] ステップＳ７０５において、鍵生成装置２００の送信部２０７は、否認可能復号鍵ＤＳＫと、複数鍵準同型復号鍵ＭＳＫから、以下の（数２）の形式で表される復号鍵ＳＫを生成する。さらに、鍵生成装置２００の送信部２０７は、否認可能暗号化鍵ＤＰＫと、複数鍵準同型暗号化鍵ＭＰＫから、以下の（数３）の形式で表される暗号化鍵ＰＫを生成する。

[0044] ＳＫ＝（ＤＳＫ，ＭＳＫ）　（数２）

ＰＫ＝（ＤＰＫ，ＭＰＫ）　（数３）

[0045] 鍵生成装置２００の送信部２０７は、暗号化鍵ＰＫを暗号化装置３００と否認乱数生成装置４００へ送信する。また、鍵生成装置２００の送信部２０７は、鍵生成装置２００の準同型演算鍵生成部２０６が生成した準同型演算鍵ＥＶＫを準同型演算装置５００へ送信する。また、鍵生成装置２００の送信部２０７は、復号鍵ＳＫを復号装置６００へ送信する。

[0046] ステップＳ７０６において、暗号化装置３００の入力部３０１は、ステップＳ７０５において鍵生成装置２００の送信部２０７が送信した暗号化鍵ＰＫを受信する。

ステップＳ７０７において、暗号化装置３００の暗号化鍵保管部３０２は、ステップＳ７０６において暗号化装置３００の入力部３０１が受信した暗号化鍵ＰＫを保管する。

[0047] ステップＳ７０８において、否認乱数生成装置４００の入力部４０１は、ステップＳ７０５において鍵生成装置２００の送信部２０７が送信した暗号化鍵ＰＫを受信する。

ステップＳ７０９において、否認乱数生成装置４００の暗号化鍵保管部４

０２は、ステップＳ７０８において否認乱数生成装置４００の入力部４０１が受信した暗号化鍵ＰＫを保管する。

[0048] ステップＳ７１０において、準同型演算装置５００の入力部５０１は、ステップＳ７０５において鍵生成装置２００の送信部２０７が送信した準同型演算鍵ＥＶＫを受信する。

ステップＳ７１１において、準同型演算装置５００の準同型演算鍵保管部５０２は、ステップＳ７１０において準同型演算装置５００の入力部５０１が受信した準同型演算鍵ＥＶＫを保管する。

[0049] ステップＳ７１２において、復号装置６００の入力部６０１は、ステップＳ７０５において鍵生成装置２００の送信部２０７が送信した復号鍵ＳＫを受信する。

ステップＳ７１３において、復号装置６００の復号鍵保管部６０２において、ステップＳ７１２において復号装置６００の入力部６０１が受信した復号鍵ＳＫを保管する。

[0050] 図８は、本実施の形態に係る秘匿情報処理システム１００の準同型演算を示すフローチャートである。

図８のステップＳ８０１からステップＳ８１５は、暗号化装置３００と準同型演算装置５００と復号装置６００とが実行する処理である。

ステップＳ８０１からステップＳ８０６は、暗号化装置３００によって実行される処理である。

ステップＳ８０７からステップＳ８１２は、準同型演算装置５００によって実行される処理である。

ステップＳ８０７からステップＳ８１５は、復号装置６００によって実行される処理である。

[0051] ステップＳ８０１において、暗号化装置３００の入力部３０１は、例えばセンサなどから収集された平文データｍ１とｍ２を受け取り、平文データｍ１とｍ２を平文保管部３０３へ送る。

ステップＳ８０２において、暗号化装置３００の平文保管部３０３は、暗

号化装置３００の入力部３０１から受け取った平文データｍ１とｍ２を保管する。

ステップＳ８０３において、暗号化装置３００の乱数生成部３０４は、乱数データｒ１とｒ２を生成し、暗号化装置３００の乱数保管部３０６へ送る。

ステップＳ８０４において、暗号化装置３００の乱数保管部３０６は、暗号化装置３００の乱数生成部３０４から受け取った乱数データｒ１とｒ２を保管する。

[0052] ステップＳ８０５において、暗号化装置３００の暗号化部３０５は、暗号化装置３００の暗号化鍵保管部３０２に保管されている否認可能暗号化鍵ＤＰＫ１と、乱数保管部３０６に保管されている乱数データｒ１と、平文保管部３０３に保管されている平文データｍ１とから暗号文データC_{DPK1}（ｍ１）を生成する。さらに、暗号化装置３００の暗号化部３０５は、暗号化装置３００の暗号化鍵保管部３０２に保管されている否認可能暗号化鍵ＤＰＫ２と、乱数保管部３０６に保管されている乱数データｒ２と、平文保管部３０３に保管されている平文データｍ２とから暗号文データC_{DPK2}（ｍ２）を生成する。暗号文データC_{DPK1}（ｍ１）とC_{DPK2}（ｍ２）を、暗号化装置３００の送信部３０７へ送る。

ステップＳ８０６において、暗号化装置３００の送信部３０７は、ステップＳ８０５において暗号化部３０５によって送られた暗号文データC_{DPK1}（ｍ１）とC_{DPK2}（ｍ２）を受け取り、準同型演算装置５００へ送信する。

[0053] ステップＳ８０７において、準同型演算装置５００の入力部５０１は、暗号化装置３００の送信部３０７から送られた暗号文データC_{DPK1}（ｍ１）とC_{DPK2}（ｍ２）を受け取り、暗号文保管部５０３へ送る。

ステップＳ８０８において、準同型演算装置５００の暗号文保管部５０３は、ステップＳ８０７において準同型演算装置５００の入力部５０１から送られた暗号文データC_{DPK1}（ｍ１）とC_{DPK2}（ｍ２）を受け取り、保管する。

ステップＳ８０９において、準同型演算装置５００の入力部５０１は、キーボードあるいはマウス、記憶装置などから入力された演算回路ｆを受け取り、演算処理構成部５０４へ送る。

ステップＳ８１０において、準同型演算装置５００の演算処理構成部５０４は、ステップＳ８０８において準同型演算装置５００の暗号文保管部５０３に保管されている暗号文データC_{DPK1}（ｍ１）とC_{DPK2}（ｍ２）と、ステップＳ８０９において準同型演算装置５００の入力部５０１から送られてきた演算回路ｆを入力として、以下の（数４）の形式で表される準同型演算処理回路Ｆを生成する。準同型演算処理回路Ｆを、準同型演算装置５００の準同型演算部５０５へ送信する。

[0054] $F(DSK1, DSK2) = f(Dec(DSK1, C_{DPK1}(m1)), Dec(DSK2, C_{DPK2}(m2)))$　（数４）

ここで、アルゴリズムＤｅｃは非特許文献１記載の復号アルゴリズムである。

準同型演算装置５００では、準同型演算時に、暗号化したまま否認可能準同型暗号の復号処理を計算することで、暗号化データを否認可能暗号文から複数鍵準同型暗号文に変換する。

[0055] ステップＳ８１１において、準同型演算装置５００の準同型演算部５０５は、準同型演算鍵ＥＶＫと、準同型演算処理回路Ｆを入力として、非特許文献２記載の準同型演算アルゴリズムを用いることで準同型演算後暗号文データ$C_{MPK}(M)$を生成し、準同型演算後暗号文データ$C_{MPK}(M)$を送信部５０６へ送る。

ステップＳ８１２において、準同型演算装置５００の送信部５０６は、準同型演算後暗号文データ$C_{MPK}(M)$を復号装置６００へ送る。

[0056] ステップＳ８１３において、復号装置６００の入力部６０１は、ステップＳ８１２において準同型演算装置５００の送信部５０６から送られた準同型演算後暗号文データ$C_{MPK}(M)$を受け取り、復号処理部６０３へ送る。

ステップＳ８１４において、復号装置６００の復号処理部６０３は、ステ

ップＳ８１３において復号装置６００の入力部６０１から送られてきた準同型演算後暗号文データC_{MPK}（Ｍ）と、復号装置６００の復号鍵保管部６０２に保管されている復号鍵ＭＳＫ１とＭＳＫ２とを用いて復号処理を行い、復号結果Ｍを得る。ここで、準同型演算後暗号文データC_{MPK}（Ｍ）の暗号化鍵集合ＭＰＫ＝｛ＭＰＫ１，ＭＰＫ２｝に対して、複数鍵準同型暗号化鍵ＭＰＫ１が複数鍵準同型復号鍵ＭＳＫ１を入力として複数鍵準同型暗号化鍵生成部２０５で生成されており、複数鍵準同型暗号化鍵ＭＰＫ２が複数鍵準同型復号鍵ＭＳＫ２を入力として複数鍵準同型暗号化鍵生成部２０５で生成されている時に限り、復号結果Ｍ＝ｆ（ｍ１，ｍ２）を復号することができる。復号処理部６０３は復号結果Ｍを復号結果保管部６０４に送る。

[0057] ステップＳ８１５において、復号装置６００の復号結果保管部６０４は、ステップＳ８１４において復号装置６００の復号処理部６０３から送られてきた復号結果Ｍを保管する。

なお、復号装置６００は、入力として準同型演算後暗号文だけを受け付ける。しかし、準同型演算前暗号文を復号したい場合は、準同型演算装置５００に、入力と同じ値をそのまま出力する演算について準同型演算を要求し、得られた準同型演算後暗号文をステップＳ８１４における処理と同様にして復号することで、準同型演算前暗号文の平文データを復号することができる。

ステップＳ８１５により、秘匿情報処理システム１００の準同型演算処理は終了する。

[0058] 図９は、本実施の形態に係る秘匿情報処理システム１００の準同型演算を示すフローチャートである。

図９のステップＳ９０１からステップＳ９０４は、暗号化装置３００と否認乱数生成装置４００とが実行する処理である。

ステップＳ９０１は、暗号化装置３００によって実行される処理である。

ステップＳ９０２からＳ９０４は、否認乱数生成装置４００によって実行される処理である。

[0059] ステップＳ９０１において、暗号化装置３００の送信部３０７は、暗号化装置３００の平文保管部３０３に保管されている平文データｍ１とｍ２と、暗号化装置３００の乱数保管部３０６に保管されている乱数データｒ１とｒ２とを否認乱数生成装置４００へ送る。

[0060] ステップＳ９０２において、否認乱数生成装置４００の入力部４０１は、ステップＳ９０１において暗号化装置３００の送信部３０７から送られてきた平文データｍ１とｍ２と、乱数データｒ１とｒ２とを受け取り、否認乱数生成装置４００の否認乱数生成部４０３へ送る。

ステップＳ９０３において、否認乱数生成装置４００の否認乱数生成部４０３は、ステップＳ９０２において否認乱数生成装置４００の入力部４０１から受け取った平文データｍ１と乱数データｒ１を受け取り、否認乱数データｒ１*を生成する。さらに、否認乱数生成装置４００の否認乱数生成部４０３は、ステップＳ９０２において否認乱数生成装置４００の入力部４０１から受け取った平文データｍ２と乱数データｒ２を受け取り、否認乱数データｒ２*を生成する。否認乱数データｒ１*とｒ２*を、否認乱数生成装置４００の否認乱数保管部４０４に送る。

ステップＳ９０４において、否認乱数生成装置４００の否認乱数保管部４０４は、Ｓ９０３において否認乱数生成装置４００の否認乱数生成部４０３から受け取った否認乱数データｒ１*とｒ２*を保管する。

[0061] 本実施の形態では、以下のような秘匿情報処理システム１００について説明した。

鍵生成装置２００は、否認可能暗号に用いられる第１否認可能暗号化鍵と第１否認可能復号鍵、および第２否認可能暗号化鍵と第２否認可能復号鍵を生成する。第１否認可能暗号化鍵と第１否認可能復号鍵、および第２否認可能暗号化鍵と第２否認可能復号鍵の各々の組は、異なるユーザにより生成される個別の鍵である。また、鍵生成装置２００は、複数鍵準同型暗号に用いられる第１複数鍵準同型暗号化鍵と第１複数鍵準同型復号鍵、および第２複数鍵準同型暗号化鍵と第２複数鍵準同型復号鍵を生成する。また、鍵生成装

置２００は、第１否認可能復号鍵と第１複数鍵準同型暗号化鍵とから第１準同型演算鍵を生成する。また、鍵生成装置２００は、第２否認可能復号鍵と第２複数鍵準同型暗号化鍵とから第２準同型演算鍵を生成する。

暗号化装置３００は、第１否認可能暗号化鍵で第１平文データを暗号化し、第１暗号化データとする。また、暗号化装置３００は、第２否認可能暗号化鍵で第２平文データを暗号化し、第２暗号化データとする。

否認乱数生成装置４００は、第１否認可能暗号化鍵と第１暗号文データとを入力とし、第１平文データの開示の否認のための第１否認乱数データを生成する。また、否認乱数生成装置４００は、第２否認可能暗号化鍵と第２暗号文データとを入力とし、第２平文データの開示の否認のための第２否認乱数データを生成する。

準同型演算装置５００は、第１準同型演算鍵と第２準同型演算鍵、および第１暗号化データと第２暗号化データを入力とし、第１平文データと第２平文データとの計算結果を準同型演算した準同型演算後暗号文データを生成する。

復号装置６００は、第１否認可能復号鍵および第２否認可能復号鍵を用いて、準同型演算後暗号文データを復号する。

[0062] ＊＊＊ハードウェア構成の説明＊＊＊

図１０は、本実施の形態に係る秘匿情報処理システム１００の各装置のハードウェア構成例を示す図である。

以下において、鍵生成装置２００と暗号化装置３００と否認乱数生成装置４００と準同型演算装置５００と復号装置６００との各装置を、秘匿情報処理システム１００の各装置と呼ぶ場合がある。

[0063] 秘匿情報処理システム１００の各装置は、コンピュータである。秘匿情報処理システム１００の各装置は、プロセッサ９１０を備えるとともに、メモリ９２１、補助記憶装置９２２、入力インタフェース９３０、出力インタフェース９４０、および通信装置９５０といった他のハードウェアを備える。プロセッサ９１０は、信号線を介して他のハードウェアと接続され、これら

他のハードウェアを制御する。

[0064] 図２から図６で説明したように、秘匿情報処理システム１００の各装置は、機能要素を備えている。

秘匿情報処理システム１００の各装置の機能要素は、ソフトウェアにより実現される。また、秘匿情報処理システム１００の各装置の記憶部は、メモリ９２１に備えられる。なお、記憶部は、補助記憶装置９２２に備えられていてもよいし、メモリ９２１と補助記憶装置９２２に分散して備えられていてもよい。

[0065] プロセッサ９１０は、秘匿情報処理プログラムを実行する装置である。秘匿情報処理プログラムは、秘匿情報処理システム１００の各装置の機能要素を実現するプログラムである。

プロセッサ９１０は、演算処理を行うＩＣである。プロセッサ９１０の具体例は、ＣＰＵ、ＤＳＰ、ＧＰＵである。ＩＣは、Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔの略語である。ＣＰＵは、Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略語である。ＤＳＰは、Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒの略語である。ＧＰＵは、Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔの略語である。

[0066] メモリ９２１は、データを一時的に記憶する記憶装置である。メモリ９２１の具体例は、ＳＲＡＭ、あるいはＤＲＡＭである。ＳＲＡＭは、Ｓｔａｔｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙの略語である。ＤＲＡＭは、Ｄｙｎａｍｉｃ Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙの略語である。

補助記憶装置９２２は、データを保管する記憶装置である。補助記憶装置９２２の具体例は、ＨＤＤである。また、補助記憶装置９２２は、ＳＤ（登録商標）メモリカード、ＣＦ、ＮＡＮＤフラッシュ、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、ＤＶＤといった可搬の記憶媒体であってもよい。なお、ＨＤＤは、Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅの略語である。ＳＤ（登録商標）は、Ｓｅｃｕｒｅ

Ｄｉｇｉｔａｌの略語である。ＣＦは、ＣｏｍｐａｃｔＦｌａｓｈ（登録商標）の略語である。ＤＶＤは、Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋの略語である。

[0067] 入力インタフェース９３０は、マウス、キーボード、あるいはタッチパネルといった入力装置と接続されるポートである。入力インタフェース９３０は、具体的には、ＵＳＢ端子である。なお、入力インタフェース９３０は、ＬＡＮと接続されるポートであってもよい。ＵＳＢは、Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓの略語である。ＬＡＮは、Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋの略語である。

[0068] 出力インタフェース９４０は、ディスプレイといった出力機器のケーブルが接続されるポートである。出力インタフェース９４０は、具体的には、ＵＳＢ端子またはＨＤＭＩ（登録商標）端子である。ディスプレイは、具体的には、ＬＣＤである。出力インタフェース９４０は、表示器インタフェースともいう。ＨＤＭＩ（登録商標）は、Ｈｉｇｈ　Ｄｅｆｉｎｉｔｉｏｎ　Ｍｕｌｔｉｍｅｄｉａ　Ｉｎｔｅｒｆａｃｅの略語である。ＬＣＤは、Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙの略語である。

[0069] 通信装置９５０は、レシーバとトランスミッタを有する。通信装置９５０は、ＬＡＮ、インターネット、電話回線、あるいはＷｉ－Ｆｉ（登録商標）といった通信網に接続している。通信装置９５０は、具体的には、通信チップまたはＮＩＣである。ＮＩＣは、Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄの略語である。

[0070] 秘匿情報処理プログラムは、秘匿情報処理システム１００において実行される。秘匿情報処理プログラムは、プロセッサ９１０に読み込まれ、プロセッサ９１０によって実行される。メモリ９２１には、秘匿情報処理プログラムだけでなく、ＯＳも記憶されている。ＯＳは、Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍの略語である。プロセッサ９１０は、ＯＳを実行しながら、秘匿情報処理プログラムを実行する。秘匿情報処理プログラムおよびＯＳは、補助記憶装置９２２に記憶されていてもよい。補助記憶装置９２２に記憶されて

いる秘匿情報処理プログラムおよびＯＳは、メモリ９２１にロードされ、プロセッサ９１０によって実行される。なお、秘匿情報処理プログラムの一部または全部がＯＳに組み込まれていてもよい。

[0071] 秘匿情報処理システム１００は、プロセッサ９１０を代替する複数のプロセッサを備えていてもよい。これら複数のプロセッサは、秘匿情報処理プログラムの実行を分担する。それぞれのプロセッサは、プロセッサ９１０と同じように、秘匿情報処理プログラムを実行する装置である。

[0072] 秘匿情報処理プログラムにより利用、処理または出力されるデータ、情報、信号値および変数値は、メモリ９２１、補助記憶装置９２２、または、プロセッサ９１０内のレジスタあるいはキャッシュメモリに記憶される。

[0073] 秘匿情報処理システム１００の各装置の機能要素の各部の「部」を「回路」、「工程」、「手順」、「処理」、あるいは「サーキットリー」に読み替えてもよい。秘匿情報処理プログラムは、秘匿情報処理システム１００の各装置の機能要素の各部の「部」を「処理」に読み替えた処理を、コンピュータに実行させる。秘匿情報処理システム１００の各装置の機能要素の各部の「部」を「プログラム」、「プログラムプロダクト」、「プログラムを記憶したコンピュータ読取可能な記憶媒体」、または「プログラムを記録したコンピュータ読取可能な記録媒体」に読み替えてもよい。また、秘匿情報処理方法は、秘匿情報処理システム１００が秘匿情報処理プログラムを実行することにより行われる方法である。

秘匿情報処理プログラムは、コンピュータ読取可能な記録媒体に格納されて提供されてもよい。また、秘匿情報処理プログラムは、プログラムプロダクトとして提供されてもよい。

[0074] ＊＊＊他の構成＊＊＊

本実施の形態では、秘匿情報処理システム１００の各装置の機能要素がソフトウェアで実現される。変形例として、秘匿情報処理システム１００の各装置の機能要素がハードウェアで実現されてもよい。

具体的には、秘匿情報処理システム１００の各装置は、プロセッサ９１０

に替えて電子回路９０９を備える。

[0075] 図１１は、本実施の形態の変形例に係る秘匿情報処理システム１００の各装置のハードウェア構成例を示す図である。

電子回路９０９は、秘匿情報処理システム１００の各装置の機能要素を実現する専用の電子回路である。電子回路９０９は、具体的には、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ロジックＩＣ、ＧＡ、ＡＳＩＣ、または、ＦＰＧＡである。ＧＡは、Ｇａｔｅ　Ａｒｒａｙの略語である。ＡＳＩＣは、Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔの略語である。ＦＰＧＡは、Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙの略語である。

[0076] 秘匿情報処理システム１００の各装置の機能要素は、１つの電子回路で実現されてもよいし、複数の電子回路に分散して実現されてもよい。

[0077] 別の変形例として、秘匿情報処理システム１００の各装置の機能要素の一部の機能が電子回路で実現され、残りの機能がソフトウェアで実現されてもよい。また、秘匿情報処理システム１００の各装置の機能要素の一部またはすべての機能がファームウェアで実現されてもよい。

[0078] プロセッサと電子回路の各々は、プロセッシングサーキットリとも呼ばれる。つまり、秘匿情報処理システム１００の各装置の機能要素は、プロセッシングサーキットリにより実現される。

[0079] ＊＊＊本実施の形態の効果の説明＊＊＊

本実施の形態に係る秘匿情報処理システムでは、例えば、以下のような効果を奏する。

通常、準同型暗号を用いたクラウドへの分析処理の委託を想定する場合、否認可能性は分析処理前の暗号文に対して成り立てば十分であり、分析処理後の暗号文は否認可能性を持つ準同型暗号の暗号文である必要はない。

本実施の形態に係る秘匿情報処理システムでは、否認可能性を持つ準同型暗号に複数鍵準同型暗号を組み合わせることで、否認可能性を担保したまま

異なる鍵で暗号化されたデータ同士でも分析処理できる機能を付与する。

本実施の形態に係る秘匿情報処理システムでは、否認可能性を持つ準同型暗号と複数鍵準同型暗号を組み合わせるために、否認可能性を持つ準同型暗号の暗号文から複数鍵準同型暗号の暗号文に変換しつつ分析処理を行う特殊な分析処理回路を設計することで、否認可能性を保ったまま異なる鍵で暗号化されたデータ同士での分析処理を可能にする。

これにより、異なる鍵で暗号化されたデータ同士で分析処理できる準同型暗号を提供できる。また、暗号化データは暗号化データ生成者の鍵だけで暗号化すれば十分であり、効率性の改善にも寄与するという効果がある。

[0080] 通常、内部で同じ鍵の下で暗号化されたデータ同士でしか準同型演算できない準同型暗号を用いて平文データを暗号化しているため、異なる鍵の下で暗号化されたデータ同士では準同型演算できなかった。本実施の形態に係る秘匿情報処理システムによれば、異なる暗号化鍵の下で生成された暗号文データ同士でも準同型演算することができる。

[0081] また、本実施の形態に係る秘匿情報処理システムによれば、異なる暗号化鍵の下で生成された暗号文データ同士で準同型演算することができるので、より小さな暗号文データサイズでクラウドサーバに分析処理を委託することができる。通常、同じ鍵の下で暗号化されたデータ同士でしか準同型演算できないため、暗号文データ作成者は自身の平文データを他の暗号文データ生成者の鍵の下でも暗号化する必要があり、暗号文データのサイズが非常に大きかった。本実施の形態に係る秘匿情報処理システムによれば、そのような他の暗号文データ生成者の鍵の下での暗号文データを生成する必要がないため、効率性の向上に寄与するという効果がある。

[0082] 以上のように、本実施の形態に係る秘匿情報処理システムによれば、否認可能暗号と複数鍵準同型暗号という二種類の暗号技術を上手く組み合わせることで、異なる鍵で暗号化されたデータ同士で分析処理できる準同型暗号を提供することができる。また、暗号化データは暗号化データ生成者の鍵だけで暗号化すれば十分であり、効率性の改善にも寄与するという効果がある。

[0083] 以上の実施の形態１では、秘匿情報処理システムの各装置の各部を独立した機能ブロックとして説明した。しかし、秘匿情報処理システムの各装置の構成は、上述した実施の形態のような構成でなくてもよい。秘匿情報処理システムの各装置の機能ブロックは、上述した実施の形態で説明した機能を実現することができれば、どのような構成でもよい。また、秘匿情報処理システムの各装置は、１つの装置でなく、複数の装置から構成されたシステムでもよい。

また、実施の形態１のうち、複数の部分を組み合わせて実施しても構わない。あるいは、この実施の形態のうち、１つの部分を実施しても構わない。その他、この実施の形態を、全体としてあるいは部分的に、どのように組み合わせて実施しても構わない。

すなわち、実施の形態１では、各実施の形態の自由な組み合わせ、あるいは各実施の形態の任意の構成要素の変形、もしくは各実施の形態において任意の構成要素の省略が可能である。

[0084] なお、上述した実施の形態は、本質的に好ましい例示であって、本開示の範囲、本開示の適用物の範囲、および本開示の用途の範囲を制限することを意図するものではない。上述した実施の形態は、必要に応じて種々の変更が可能である。例えば、フロー図あるいはシーケンス図を用いて説明した手順は、適宜に変更してもよい。

符号の説明

[0085] １００　秘匿情報処理システム、１０１　インターネット、２００　鍵生成装置、２０１，３０１，４０１，５０１，６０１　入力部、２０２　否認可能復号鍵生成部、２０３　否認可能暗号化鍵生成部、２０４　複数鍵準同型復号鍵生成部、２０５　複数鍵準同型暗号化鍵生成部、２０６　準同型演算鍵生成部、２０７，３０７，５０６　送信部、３００　暗号化装置、３０２，４０２　暗号化鍵保管部、３０３　平文保管部、３０４　乱数生成部、３０５　暗号化部、３０６　乱数保管部、４００　否認乱数生成装置、４０３　否認乱数生成部、４０４　否認乱数保管部、５００　準同型演算装置、

５０２　準同型演算鍵保管部、５０３　暗号文保管部、５０４　演算処理構成部、５０５　準同型演算部、６００　復号装置、６０２　復号鍵保管部、６０３　復号処理部、６０４　復号結果保管部、９０９　電子回路、９１０　プロセッサ、９２１　メモリ、９２２　補助記憶装置、９３０　入力インタフェース、９４０　出力インタフェース、９５０　通信装置。

請求の範囲

[請求項1] 暗号化鍵と復号鍵と準同型演算鍵を生成する鍵生成装置と、

暗号化鍵で平文データを暗号化した暗号化データを生成する暗号化装置と、

暗号化鍵と暗号文データとを入力とし、平文データの開示の否認のための否認乱数データを生成する否認乱数生成装置と、

準同型演算鍵と暗号化データとを入力とし、平文データの計算結果を準同型演算した準同型演算後暗号文データを生成する準同型演算装置と、

準同型演算後暗号文データを復号する復号装置と

を備えた秘匿情報処理システム。

[請求項2] 前記鍵生成装置は、

前記暗号化鍵として、否認可能暗号に用いる否認可能暗号化鍵と複数鍵準同型暗号に用いる複数鍵準同型暗号化鍵とを出力する請求項１に記載の秘匿情報処理システム。

[請求項3] 前記鍵生成装置は、

前記復号鍵として、否認可能暗号に用いる否認可能復号鍵と複数鍵準同型暗号に用いる複数鍵準同型復号鍵を出力する請求項２に記載の秘匿情報処理システム。

[請求項4] 前記鍵生成装置は、

前記準同型演算鍵として、前記否認可能復号鍵を複数鍵準同型暗号で暗号化した複数鍵準同型暗号文を出力する請求項３に記載の秘匿情報処理システム。

[請求項5] 前記準同型演算装置は、

準同型演算時に、暗号化したまま否認可能準同型暗号の復号処理を計算することで、暗号化データを否認可能暗号文から複数鍵準同型暗号文に変換する請求項４に記載の秘匿情報処理システム。

[請求項6] 鍵生成装置が、暗号化鍵と復号鍵と準同型演算鍵を生成し、

暗号化装置が、暗号化鍵で平文データを暗号化した暗号化データを生成し、

否認乱数生成装置が、暗号化鍵と暗号文データとを入力とし、平文データの開示の否認のための否認乱数データを生成し、

準同型演算装置が、準同型演算鍵と暗号化データとを入力とし、平文データの計算結果を準同型演算した準同型演算後暗号文データを生成し、

復号装置が、準同型演算後暗号文データを復号する秘匿情報処理システムに用いられる秘匿情報処理方法。

[請求項7] 暗号化鍵と復号鍵と準同型演算鍵を生成する鍵生成処理と、

暗号化鍵で平文データを暗号化した暗号化データを生成する暗号化処理と、

暗号化鍵と暗号文データとを入力とし、平文データの開示の否認のための否認乱数データを生成する否認乱数生成処理と、

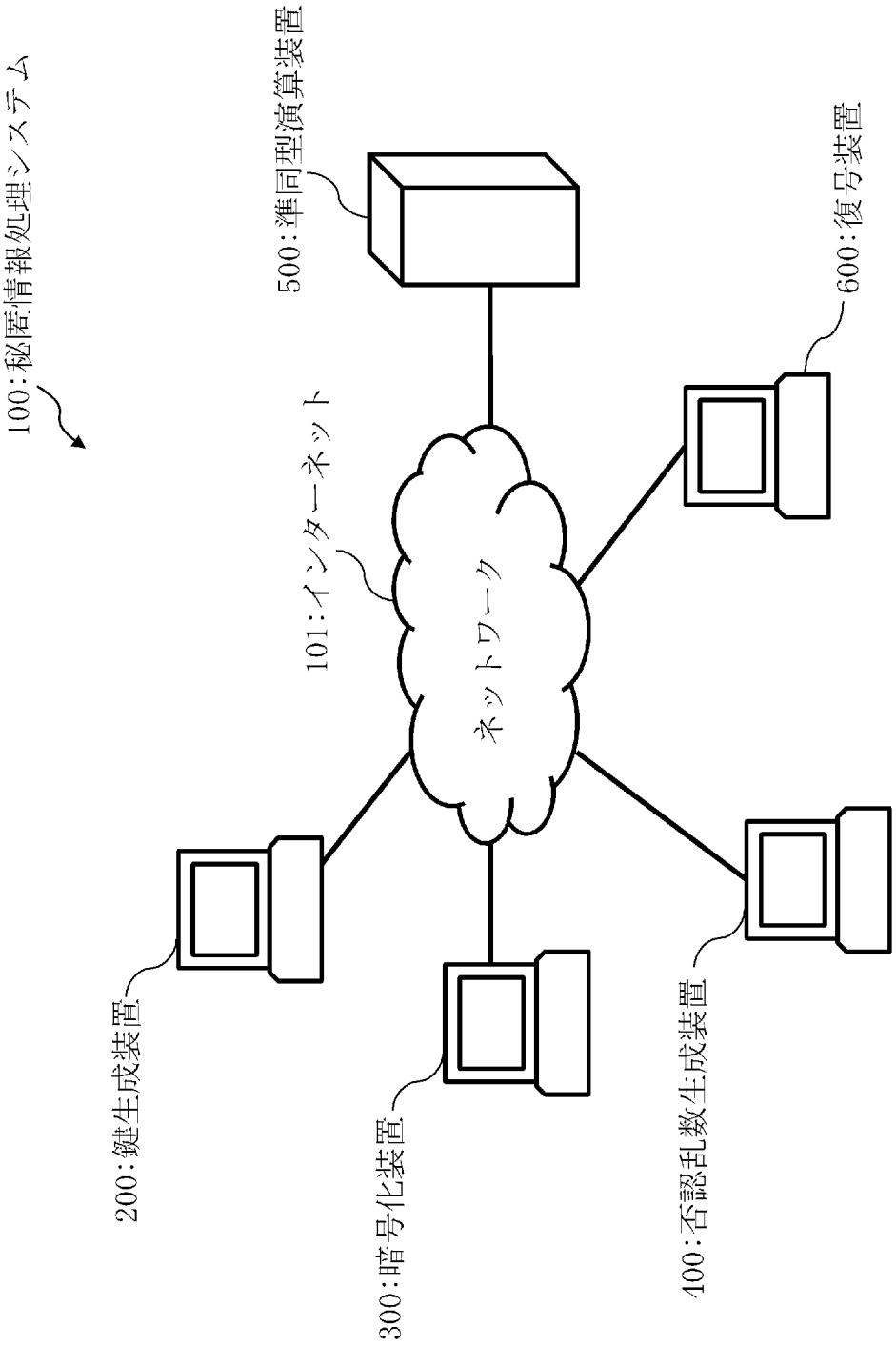
準同型演算鍵と暗号化データとを入力とし、平文データの計算結果を準同型演算した準同型演算後暗号文データを生成する準同型演算処理と、

準同型演算後暗号文データを復号する復号処理と

をコンピュータに実行させる秘匿情報処理プログラム。

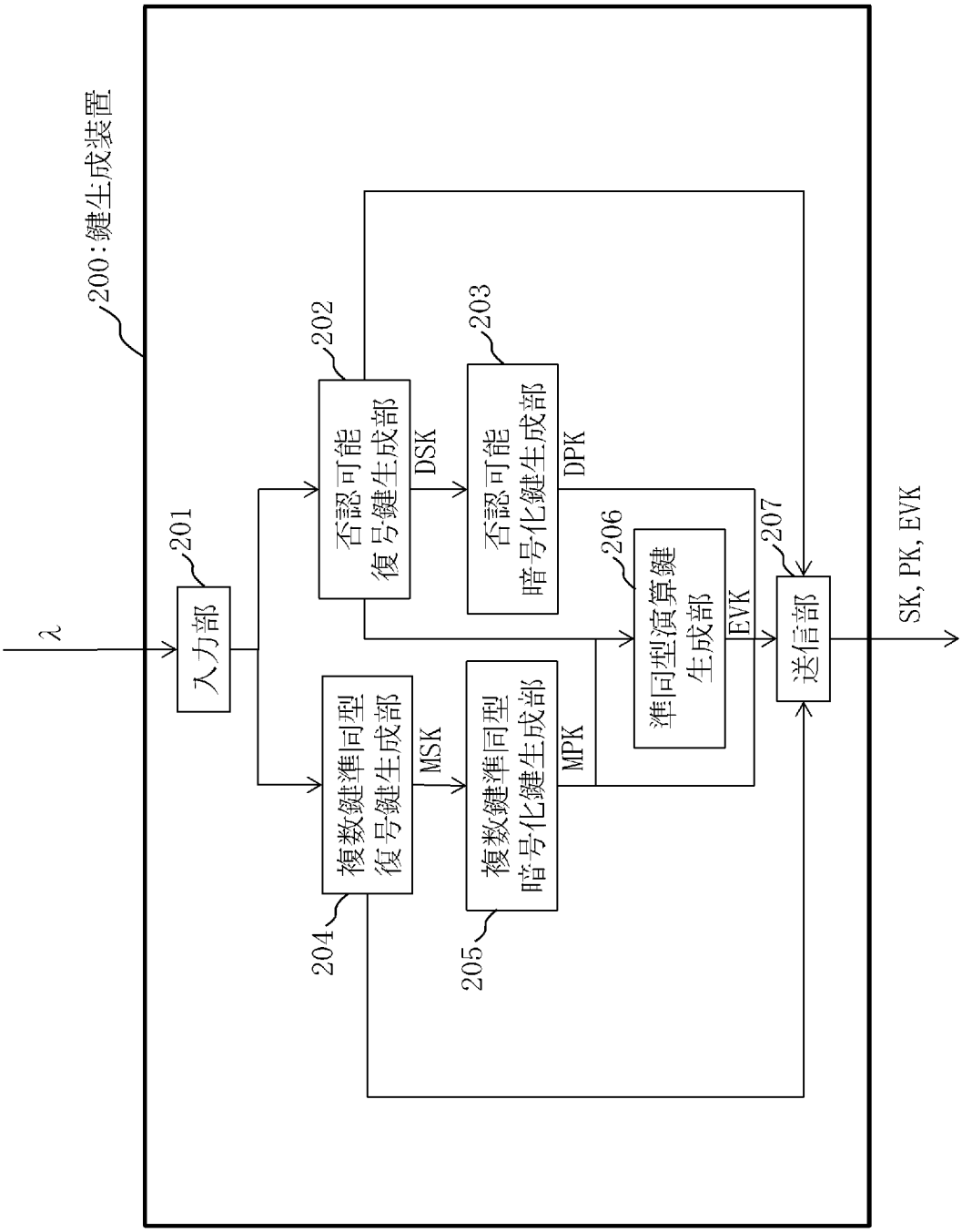
[図1]

図1


100:秘匿情報処理システム
500:準同型演算装置
600:復号装置
101:インターネット
ネットワーク
200:鍵生成装置
300:暗号化装置
100:否認乱数生成装置

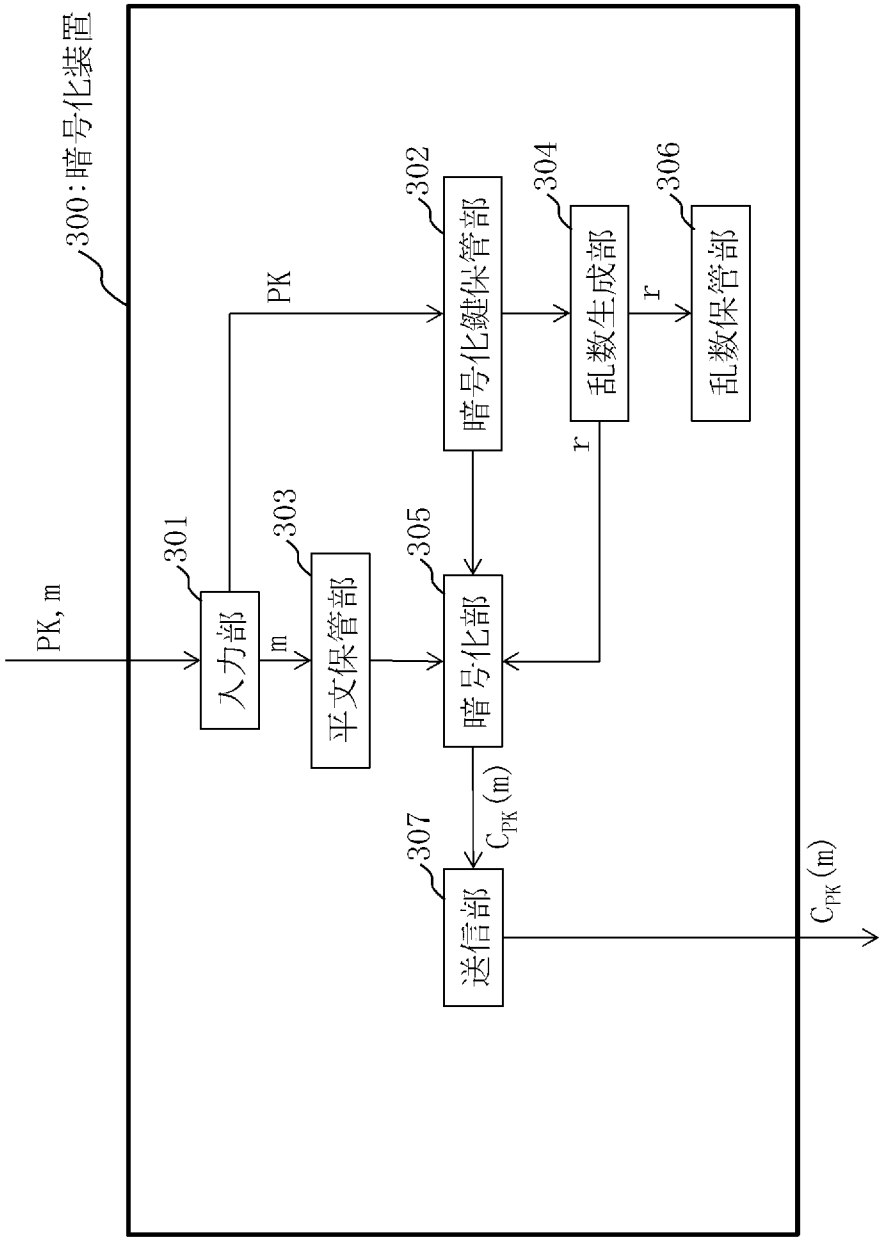
[図2]

図2


200：鍵生成装置
λ
201
入力部
202
否認可能
復号鍵生成部
DSK
203
否認可能
暗号化鍵生成部
DPK
204
複数鍵準同型
復号鍵生成部
MSK
205
複数鍵準同型
暗号化鍵生成部
MPK
206
準同型演算鍵
生成部
EVK
207
送信部
SK, PK, EVK

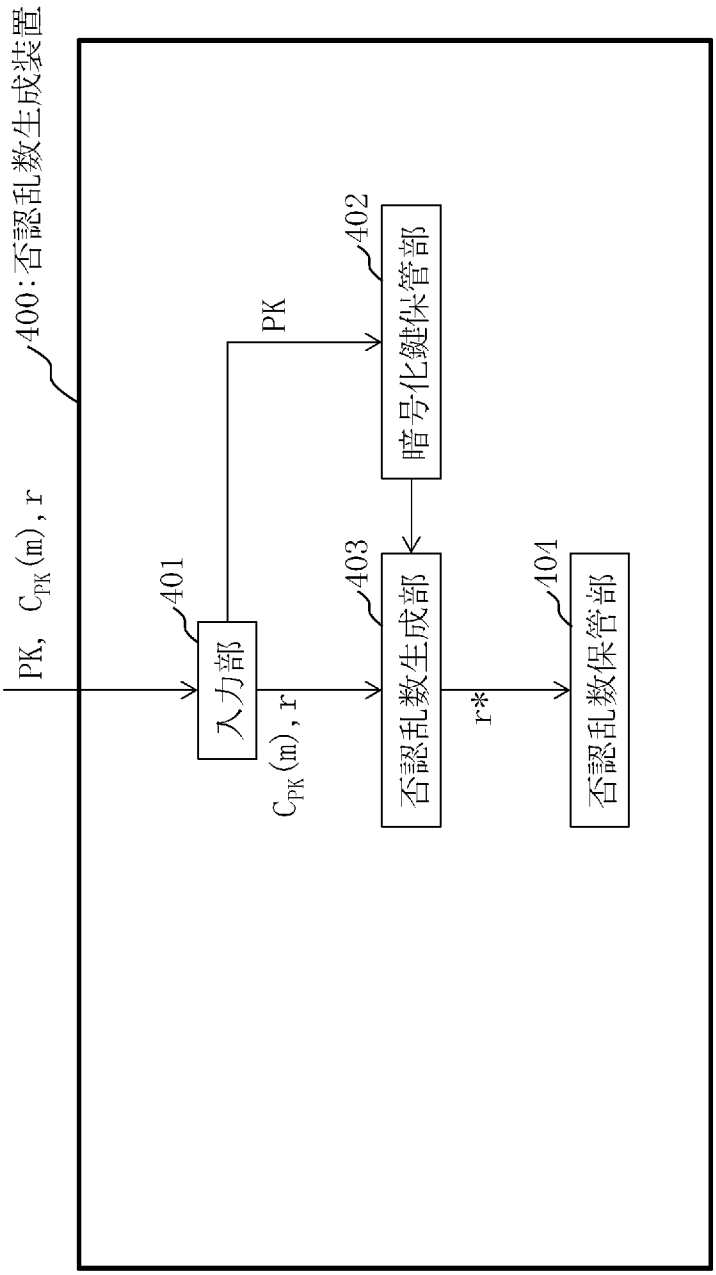
[図3]

図3


300：暗号化装置
PK, m
301
入力部
PK
m
303
平文保管部
302
暗号化鍵保管部
304
乱数生成部
306
乱数保管部
r
r
305
暗号化部
C_{PK} (m)
307
送信部
C_{PK} (m)

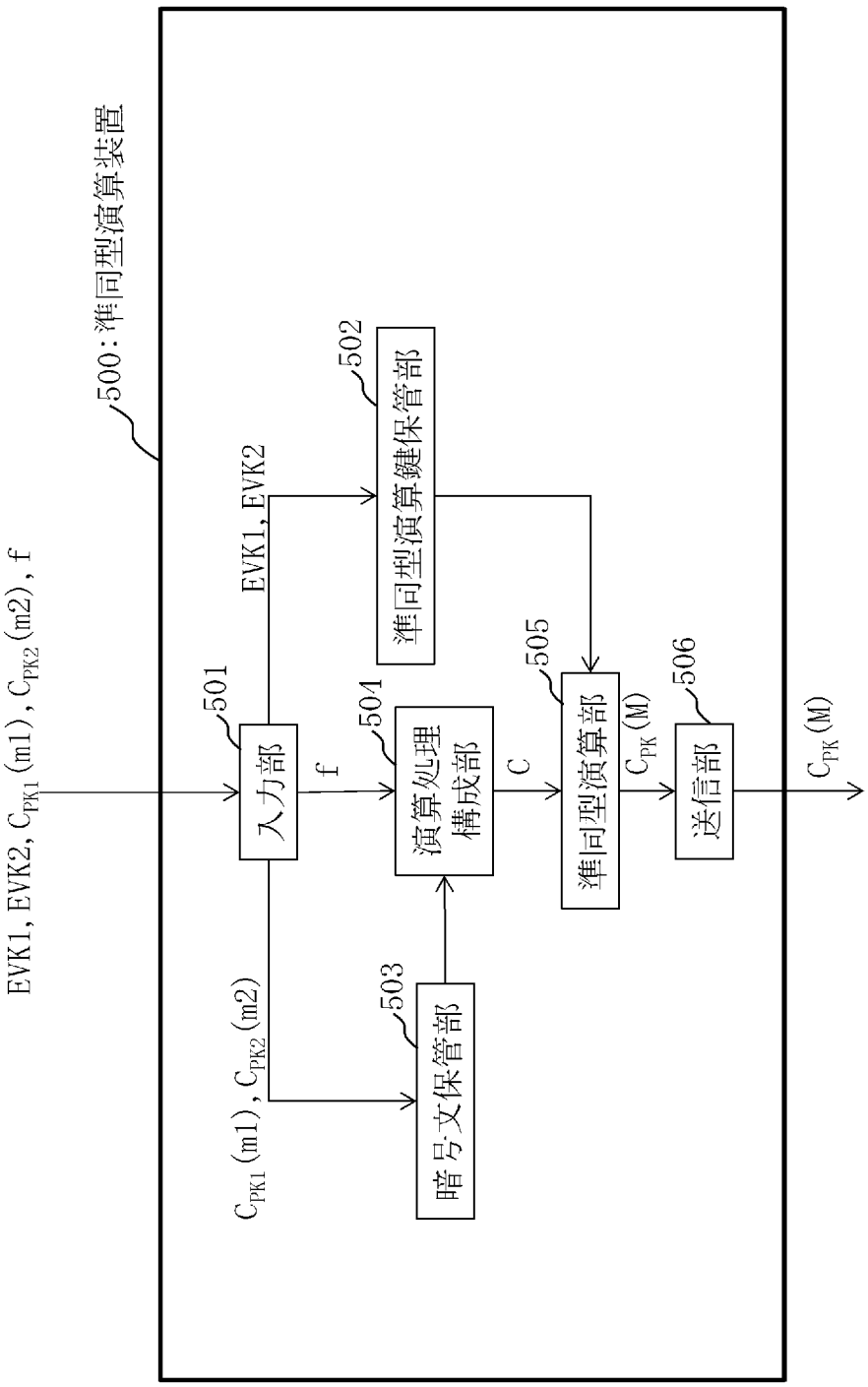
[図4]

図4


400：否認乱数生成装置
PK, $C_{PK}(m)$, r
401
入力部
PK
402
暗号化鍵保管部
$C_{PK}(m)$, r
403
否認乱数生成部
r*
404
否認乱数保管部

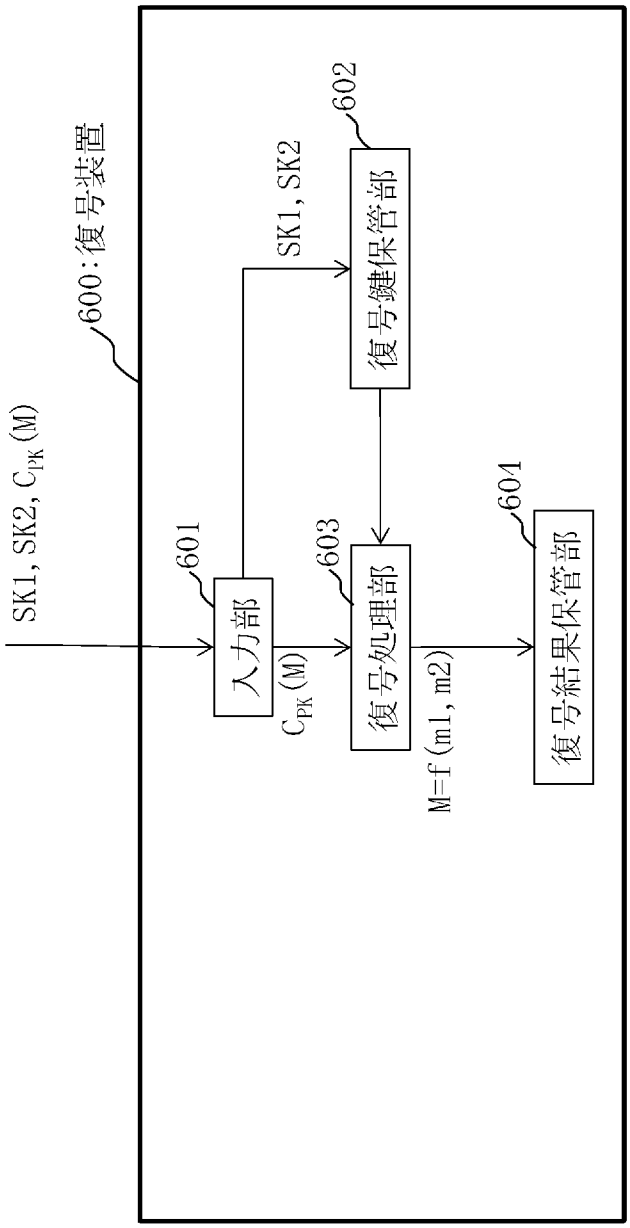
[図5]

図5


500:準同型演算装置
EVK1, EVK2, C_{PK1}(m1), C_{PK2}(m2), f
501
入力部
EVK1, EVK2
502
準同型演算鍵保管部
504
演算処理構成部
f
C
505
準同型演算部
C_{PK}(M)
506
送信部
C_{PK}(M)
503
暗号文保管部
C_{PK1}(m1), C_{PK2}(m2)

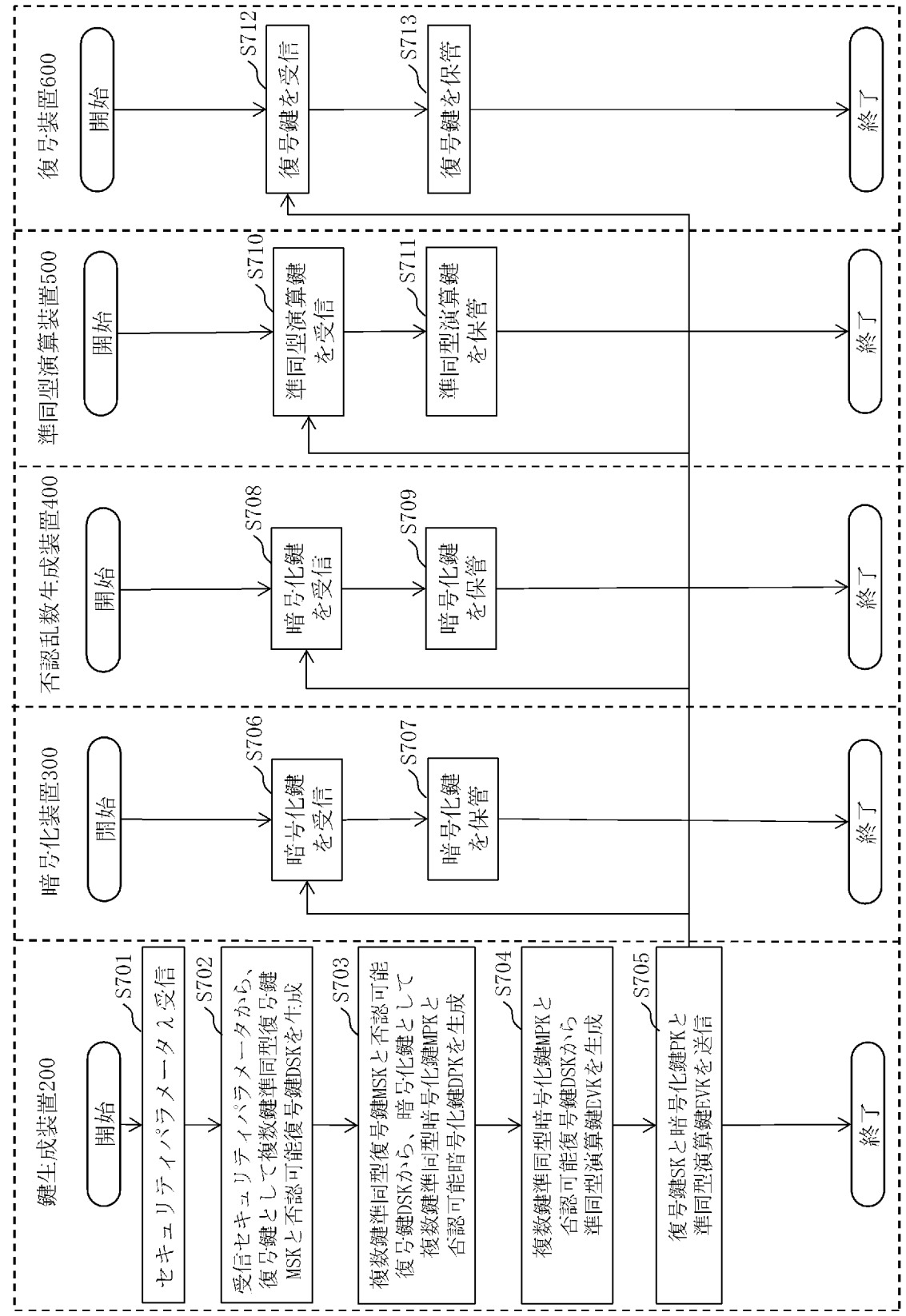
[図6]

図6


600:復号装置
SK1, SK2, C_{PK}(M)
601
入力部
SK1, SK2
602
復号鍵保管部
603
復号処理部
C_{PK}(M)
M=f(m1, m2)
604
復号結果保管部

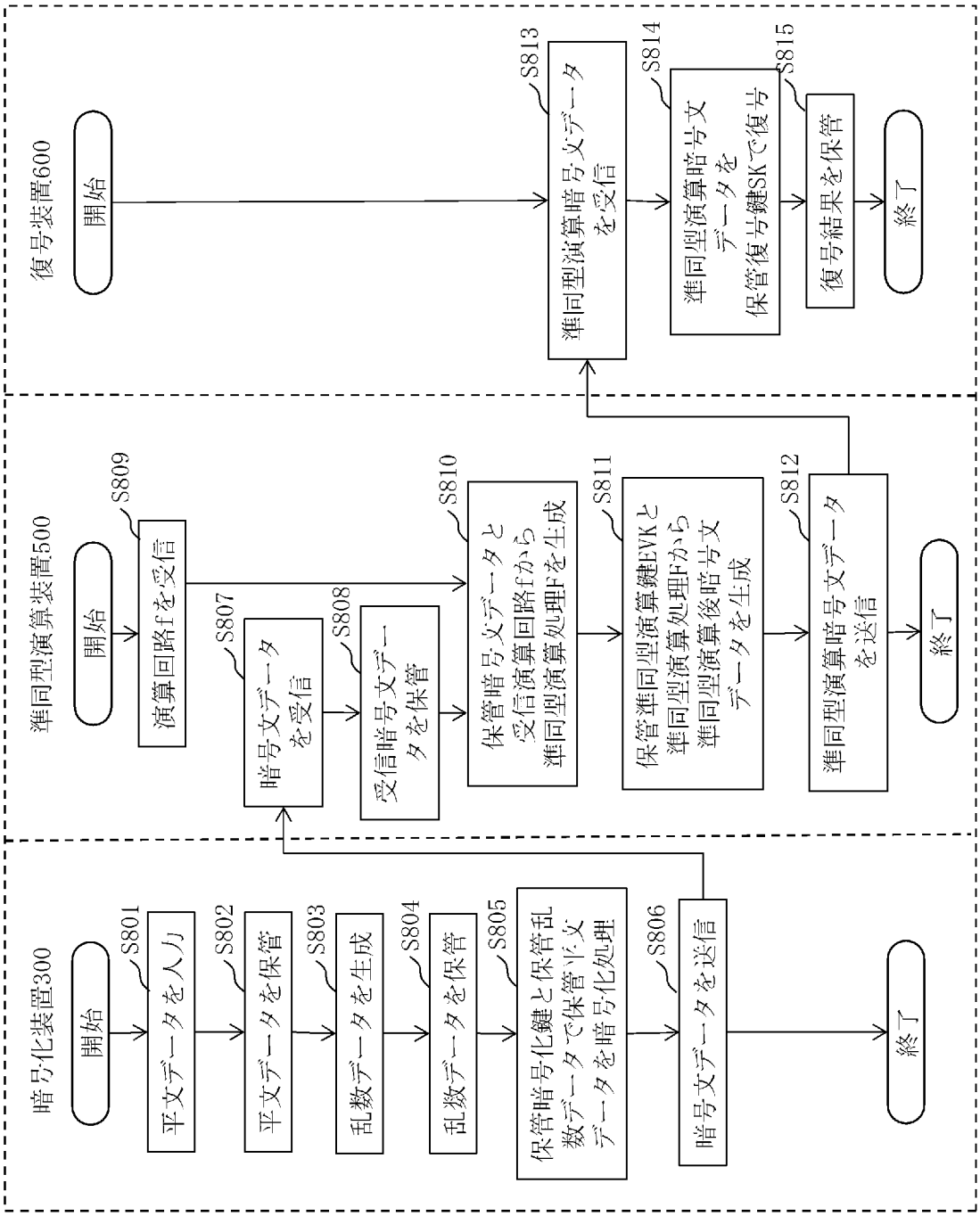
[図7]

図7


鍵生成装置200
開始
S701
セキュリティパラメータλ受信
S702
受信セキュリティパラメータから、
復号鍵として複数鍵準同型復号鍵
MSKと否認可能復号鍵DSKを生成
S703
複数鍵準同型復号鍵MSKと否認可能
復号鍵DSKから、暗号化鍵として
複数鍵準同型暗号化鍵MPKと
否認可能暗号化鍵DPKを生成
S704
複数鍵準同型暗号化鍵MPKと
否認可能復号鍵DSKから
準同型演算鍵EVKを生成
S705
復号鍵SKと暗号化鍵PKと
準同型演算鍵EVKを送信
終了
暗号化装置300
開始
S706
暗号化鍵
を受信
S707
暗号化鍵
を保管
終了
否認乱数生成装置400
開始
S708
暗号化鍵
を受信
S709
暗号化鍵
を保管
終了
準同型演算装置500
開始
S710
準同型演算鍵
を受信
S711
準同型演算鍵
を保管
終了
復号装置600
開始
S712
復号鍵を受信
S713
復号鍵を保管
終了

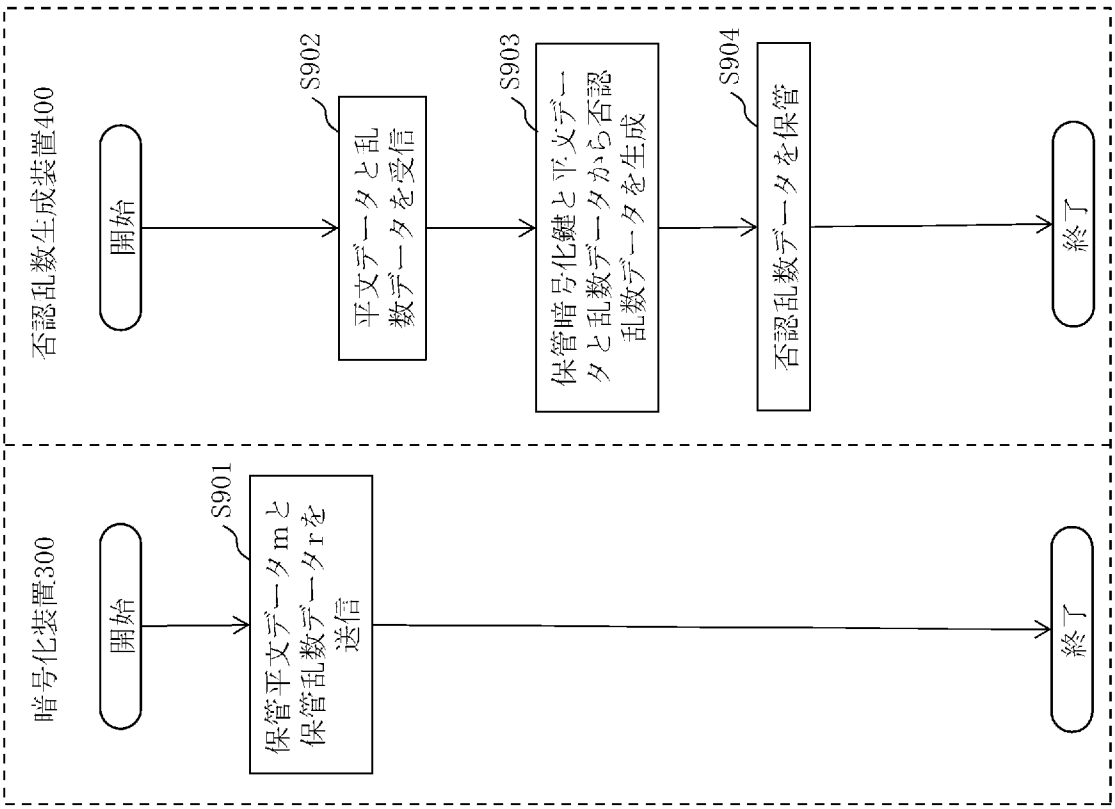
[図8]

図8


暗号化装置300
開始
S801
平文データを入力
S802
平文データを保管
S803
乱数データを生成
S804
乱数データを保管
S805
保管暗号化鍵と保管乱数データで保管平文データを暗号化処理
S806
暗号文データを送信
終了
準同型演算装置500
開始
S809
演算回路fを受信
S807
暗号文データを受信
S808
受信暗号文データを保管
S810
保管暗号文データと受信演算回路fから準同型演算処理Fを生成
S811
保管準同型演算鍵EVKと準同型演算処理Fから準同型演算後暗号文データを生成
S812
準同型演算暗号文データを送信
終了
復号装置600
開始
S813
準同型演算暗号文データを受信
S814
準同型演算暗号文データを保管復号鍵SKで復号
S815
復号結果を保管
終了

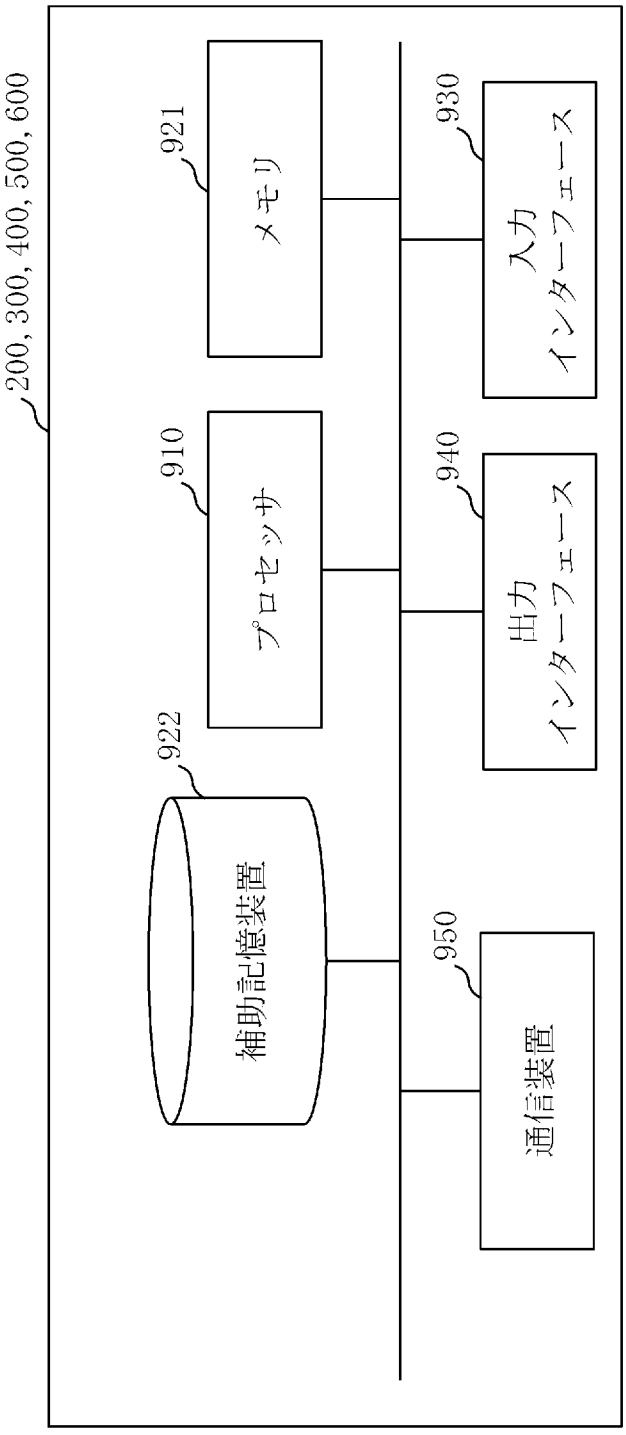
[図9]

図9


否認乱数生成装置400
開始
S902
平文データと乱数データを受信
S903
保管暗号化鍵と平文データと乱数データから否認乱数データを生成
S904
否認乱数データを保管
終了
暗号化装置300
開始
S901
保管平文データmと保管乱数データrを送信
終了

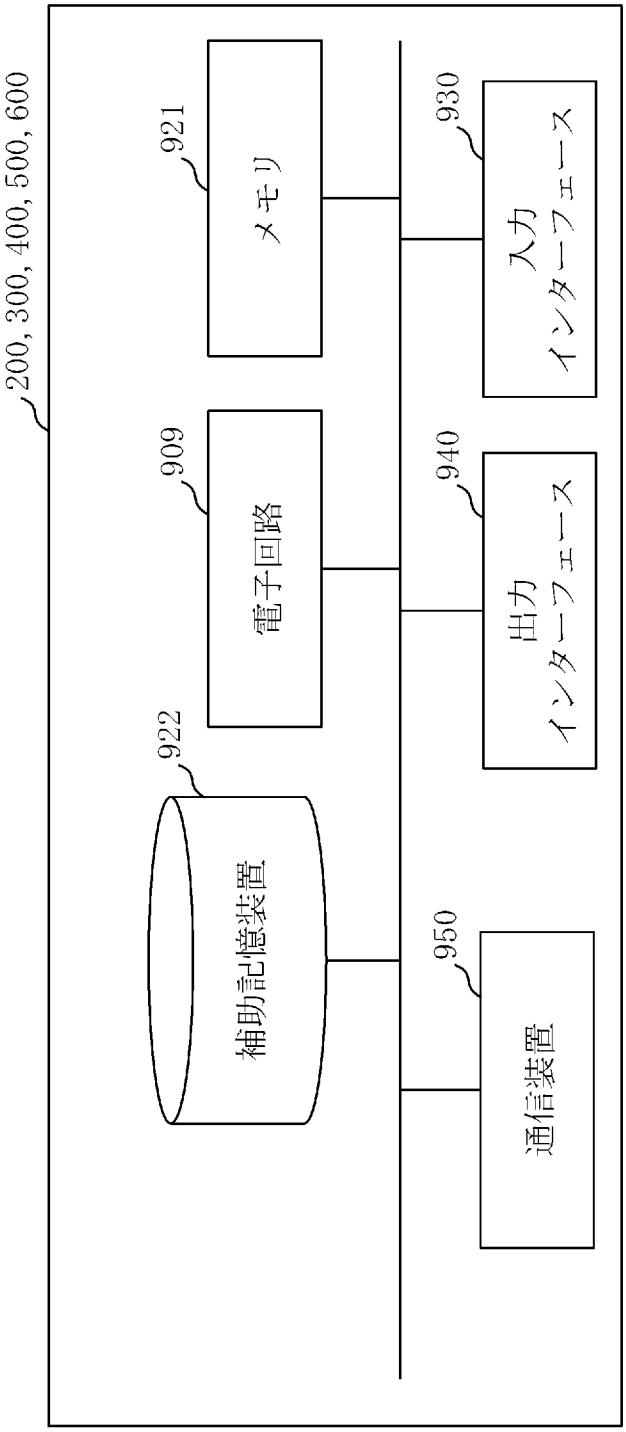
[図10]

図10


200, 300, 400, 500, 600
910
プロセッサ
921
メモリ
922
補助記憶装置
930
入力
インターフェース
940
出力
インターフェース
950
通信装置

[図11]

図11


200, 300, 400, 500, 600
921
メモリ
930
入力
インターフェース
909
電子回路
940
出力
インターフェース
922
補助記憶装置
950
通信装置

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/012095

A. CLASSIFICATION OF SUBJECT MATTER

G09C 1/00(2006.01)i
FI: G09C1/00 650Z

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)

G09C1/00

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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.
A	AGRAWAL, Shweta et al. Deniable fully homomorphic encryption from LWE. Cryptology ePrint Archive [online]. November 2021 [retrieved on 08 May 2023], paper 2020/1588, version 20211112:234815, pp. 1-45, Retrieved from the Internet: <URL: https://eprint.iacr.org/archive/2020/1588/20211112:234815> pp. 16-18 "2.2 Deniable Homomorphic Encryption"	1-7
A	LOPEZ-ALT, Adriana et al. On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption. Proceedings of the forty-fourth annual ACM symposium on Theory of computing [online]. 2012 [retrieved on 08 May 2023], pp. 1219-1234, Retrieved from the Internet: <URL: https://dl.acm.org/doi/abs/10.1145/2213977.2214086> pp. 1221-1223 "1.1 Our Results and Techniques"	1-7
A	BRAKERSKI, Zvika et al. Lattice-Based Fully Dynamic Multi-Key FHE with Short Ciphertexts. Cryptology ePrint Archive [online]. November 2016 [retrieved on 08 May 2023], paper 2016/339, version 20161118:093848, pp. 1-23, Retrieved from the Internet: <URL: https://eprint.iacr.org/archive/2016/339/20161118:093848> p. 8 "2.2 Multi-Key Homomorphic Encryption"	1-7

☑ 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	Date of mailing of the international search report
08 May 2023	**23 May 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/012095

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	安田 聖　ほか, 複数鍵準同型代理人再暗号, ２０１８年暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１８）, January 2018, 1A2-5, pp. 1-8, (2018 Symposium on Cryptography and Information Security), non-official translation (YASUDA, Satoshi et al. Multi-key homomorphic proxy re-encryption.) pp. 4-7, "4 MH-PRE configuration"	1-7

国際調査報告

国際出願番号
PCT/JP2023/012095

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G09C 1/00(2006.01)i
FI: G09C1/00 650Z

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（ＩＰＣ））

G09C1/00

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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３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
A	AGRAWAL, Shweta et al., Deniable fully homomorphic encryption from LWE, Cryptology ePrint Archive [online], 2021.11 [retrieved on 2023.05.08], Paper 2020/1588, version 20211112:234815, p.1-45, Retrieved from the Internet: <URL: https://eprint.iacr.org/archive/2020/1588/20211112:234815> p.16-18 「2.2 Deniable Homomorphic Encryption」	1-7
A	LOPEZ-ALT, Adriana et al., On-the-Fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption, Proceedings of the forty-fourth annual ACM symposium on Theory of computing [online], 2012 [retrieved on 2023.05.08], p.1219-1234, Retrieved from the Internet: <URL: https://dl.acm.org/doi/abs/10.1145/2213977.2214086> p.1221-1223 「1.1 Our Results and Techniques」	1-7
A	BRAKERSKI, Zvika et al., Lattice-Based Fully Dynamic Multi-Key FHE with Short Ciphertexts, Cryptology ePrint Archive [online], 2016.11 [retrieved on 2023.05.08], Paper 2016/339, version 20161118:093848, p.1-23, Retrieved from the Internet: <URL: https://eprint.iacr.org/archive/2016/339/20161118:093848> p.8 「2.2 Multi-Key Homomorphic Encryption」	1-7

☑ 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抵触するものではなく、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	国際調査報告の発送日
08.05.2023	23.05.2023

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
金沢　史明 5S 2674
電話番号 03-3581-1101 内線 3545

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
A	安田 聖　ほか，複数鍵準同型代理人再暗号，２０１８年 暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１８），2018.01，1A2-5，p.1-8 p.4-7 「4 MH-PREの構成」	1-7