

(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
2017年9月28日(28.09.2017)



(10) 国際公開番号

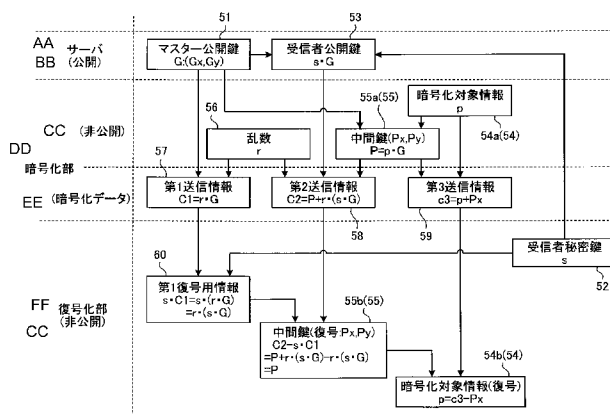
WO 2017/163434 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) H04L 9/30 (2006.01)
H04L 9/16 (2006.01)
- (21) 国際出願番号: PCT/JP2016/059771
- (22) 国際出願日: 2016年3月25日(25.03.2016)
- (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: 中国電力株式会社 (THE CHUGOKU ELECTRIC POWER CO., INC.) [JP/JP]; 〒7308701 広島県広島市中区小町4番33号 Hiroshima (JP).
- (72) 発明者: 芳野 達哉 (YOSHINO, Tatsuya); 〒7308701 広島県広島市中区小町4番33号 中国電力株式会社内 Hiroshima (JP). 板井 政行 (ITAI, Masayuki); 〒7308701 広島県広島市中区小町4番33号 中国電力株式会社内 Hiroshima (JP).
- (74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関3丁目8番1号 虎の門三井ビルディング 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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,

[続葉有]

(54) Title: INFORMATION PROCESSING METHOD AND INFORMATION PROCESSING SYSTEM

(54) 発明の名称: 情報処理方法及び情報処理システム



- 51 Master public key
52 Recipient private key
53 Recipient public key
54a(54) Cipher target information
54b(54) Cipher target information (decoding)
55a(55) Intermediate key
55b(55) Intermediate key (decoding Px, Py)
56 Random number
57 First transmission information
58 Second transmission information
59 Third transmission information
60 First decoding information
AA Server
BB Disclosed
CC Undisclosed
DD Cipher unit
EE Ciphered data
FF Decoding unit

(57) Abstract: An information processing method has: a step for setting a master public key indicating coordinates on an elliptic curve; a step for generating a recipient public key indicating the product of a recipient secret key that is undisclosed information and the master public key; a step for generating an intermediate key indicating the product of cipher target information that is undisclosed information and the master public key; a step for generating first transmission information indicating the product of a random number that is undisclosed information and the master public key; a step for generating second transmission information indicating the addition of the product of the random number and the recipient public key and the intermediate key; a step for generating third transmission information derived from calculation using at least the cipher target information and information indicated by the intermediate key; a step for generating first decoding information that is the product of the recipient secret key and the first transmission information; a step for acquiring the intermediate key by subtracting the first decoding information from the second transmission information; and a step for acquiring the cipher target information on the basis of the intermediate key and the third transmission information.

(57) 要約:

[続葉有]

WO 2017/163434 A1



ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, 添付公開書類:

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).

— 国際調査報告 (条約第 21 条(3))

情報処理方法は、楕円曲線上の座標を示すマスター公開鍵の設定工程、非公開情報である受信者秘密鍵とマスター公開鍵との積を示す受信者公開鍵を生成する工程、非公開情報である暗号化対象情報とマスター公開鍵との積を示す中間鍵を生成する工程、非公開情報である乱数とマスター公開鍵との積を示す第 1 送信情報を生成する工程、乱数と受信者公開鍵との積と、中間鍵との加算を示す第 2 送信情報を生成する工程、少なくとも暗号化対象情報及び中間鍵が示す情報を用いた演算によって導出される第 3 送信情報を生成する工程、受信者秘密鍵と第 1 送信情報との積である第 1 復号用情報を生成する工程、第 2 送信情報から第 1 復号用情報を減じて中間鍵を得る工程、及び、中間鍵と第 3 送信情報に基づいて暗号化対象情報を得る工程を有する。

明 細 書

発明の名称： 情報処理方法及び情報処理システム

技術分野

[0001] 本発明は、情報処理方法及び情報処理システムに関する。

背景技術

[0002] コンピュータの利用者間で伝送されるデータの機密性を高める目的で、データを暗号化して送信し、受信者が復号化する方法が知られている（例えば、特許文献1）。

先行技術文献

特許文献

[0003] 特許文献1：特開2005-242993号公報

発明の概要

発明が解決しようとする課題

[0004] 暗号化されたデータの復号化には、暗号化に用いられたパスワード等、鍵として機能するデータが必要になる。パスワードを用いる方法は簡便であるが、パスワードを受信者に知らせる必要があり、パスワードの漏えいが問題になることがある。

[0005] 本発明では、より高い機密性を確保することができる情報処理方法及び情報処理システ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

[0006] 上述した課題を解決し、目的を達成するために、本発明は、非公開情報である暗号化対象情報を取り扱う情報処理装置による情報処理方法であって、楕円曲線上の座標を示す公開情報であるマスター公開鍵の設定工程と、非公開情報である受信者秘密鍵と前記マスター公開鍵との積を示す公開情報である受信者公開鍵を生成する工程と、非公開情報である暗号化対象情報と前記マスター公開鍵との積を示す非公開情報である中間鍵を生成する工程と、非公開情報である乱数と前記マスター公開鍵との積を示す第1送信情報を生成

する工程と、前記乱数と前記受信者公開鍵との積と、前記中間鍵との加算を示す第2送信情報を生成する工程と、少なくとも暗号化対象情報及び前記中間鍵が示す情報を用いた演算によって導出される第3送信情報を生成する工程と、前記受信者秘密鍵と前記第1送信情報との積である第1復号用情報を生成する工程と、前記第2送信情報から前記第1復号用情報を減じて前記中間鍵を得る工程と、前記中間鍵と前記第3送信情報に基づいて前記暗号化対象情報を得る工程とを有する。

[0007] 本発明の望ましい態様として、前記第3送信情報は、前記中間鍵が示すx座標と前記暗号化対象情報との加算である。

[0008] 本発明の望ましい態様として、前記第3送信情報は、前記第1送信情報が示すx座標と前記中間鍵が示すx座標との積と、前記第1送信情報が示すy座標と前記中間鍵が示すy座標との積とが前記暗号化対象情報に付加された情報である。

[0009] 本発明の望ましい態様として、前記中間鍵が示すx座標を P_x とし、前記中間鍵が示すy座標を P_y とし、前記第1送信情報が示すx座標を $C1_x$ とし、前記第1送信情報が示すy座標を $C1_y$ とし、前記第2送信情報が示すx座標を $C2_x$ とし、前記第2送信情報が示すy座標を $C2_y$ とし、前記第3送信情報を $c3$ とし、前記暗号化対象情報を p とすると、式(1)が成立する。

$$c3 = (C1_x^{P_x} \bmod C2_x) + (C1_y^{P_y} \bmod C2_y) + p \cdots (1)$$

[0010] また、上述した課題を解決し、目的を達成するために、本発明は、情報の送信者及び情報の受信者が操作する1つ以上の端末と、前記端末と通信可能に接続されたサーバとを有し、前記送信者から前記受信者宛てに送信される非公開情報である暗号化対象情報を暗号化する情報処理システムであって、前記サーバは、楕円曲線上の座標を示す公開情報であるマスター公開鍵及び非公開情報である受信者秘密鍵と前記マスター公開鍵との積を示す公開情報である受信者公開鍵を記憶する第1記憶部を備え、前記端末又は前記サーバ

は、前記暗号化対象情報と前記マスター公開鍵との積を示す非公開情報である中間鍵を生成する中間鍵生成部と、非公開情報である乱数と前記マスター公開鍵との積を示す第1送信情報、前記乱数と前記受信者公開鍵との積と前記中間鍵との加算を示す第2送信情報、少なくとも暗号化対象情報及び前記中間鍵が示す情報を用いた演算によって導出される第3送信情報を生成する暗号化部と、前記受信者秘密鍵と前記第1送信情報との積である第1復号用情報を算出し、前記第2送信情報から前記第1復号用情報を減じて前記中間鍵を導出し、導出された前記中間鍵と前記第3送信情報に基づいて前記暗号化対象情報を得る復号化部とを備える。

[0011] 本発明の望ましい態様として、前記送信者の端末は、前記中間鍵生成部及び前記暗号化部を備え、前記受信者の端末は、前記復号化部と、前記受信者秘密鍵を記憶する第2記憶部とを備え、前記送信者の端末は、前記第1送信情報、前記第2送信情報及び前記第3送信情報を前記サーバに送信し、前記サーバは、前記第1送信情報、前記第2送信情報及び前記第3送信情報を前記受信者の端末に送信する。

発明の効果

[0012] 本発明によれば、より高い機密性を確保することができる。

図面の簡単な説明

[0013] [図1]図1は、本発明の一実施形態に係る情報処理システムの主要構成を示すブロック図である。

[図2]図2は、暗号化及び復号化に係る各種のデータの関係を模式的に示す図である。

[図3]図3は、暗号化対象情報を暗号化して電子メールで送信する場合の例を模式的に示す図である。

[図4]図4は、図2に示す各種のデータが取り得る具体的な形式の一例及び楕円曲線の方程式の一例を示す図である。

[図5]図5は、楕円曲線の一例を示す図である。

[図6]図6は、受信者による準備処理の流れの一例を示すフローチャートであ

る。

[図7]図7は、送信者による暗号化処理及びデータの送信に係る処理の流れの一例を示すフローチャートである。

[図8]図8は、受信者による復号化処理の流れの一例を示すフローチャートである。

発明を実施するための形態

[0014] 次に、本発明の実施形態を、図面を参照して詳細に説明する。図1は、本発明の一実施形態に係る情報処理システムの主要構成を示すブロック図である。図2は、暗号化及び復号化に係る各種のデータの間関係を模式的に示す図である。図3は、暗号化対象情報を暗号化して電子メールで送信する場合の例を模式的に示す図である。図4は、図2に示す各種のデータが取り得る具体的な形式の一例及び楕円曲線の方程式の一例を示す図である。情報処理システムは、情報の送信者（以下、単に送信者）及び情報の受信者（以下、単に受信者）が操作する1つ以上の端末20と、端末20と通信可能に接続されたサーバ10とを有し、送信者から受信者宛てに送信される非公開情報である暗号化対象情報54（p）を暗号化する情報処理システムである。なお、公開情報とは、送信者及び受信者以外の第三者が取得することができ、その情報の内容を把握可能な情報をさす。非公開情報とは、送信者及び受信者以外の第三者による情報の取得及び情報の内容の把握がなされるべきでない情報をさす。

[0015] サーバ10は、演算部11、記憶部12、通信部13等を備える。演算部11は、CPU（Central Processing Unit）等の演算装置を有し、記憶部12に記憶されているソフトウェア・プログラム及び係るソフトウェア・プログラムが参照するデータ（以下、プログラム等）を読み出して実行処理し、情報処理システムの動作に係る各種の処理を行う。記憶部12は、例えば半導体メモリ、ハードディスクドライブ等、各種の記憶装置を有し、図示しないプログラム等を記憶する。通信部13は、ネットワークインタフェースコントローラ（NIC：Network Interface Controller）、通信回線Nに接

続するためのインタフェース等を有し、通信回線Nを介して接続された端末20との間で行われる通信に係る各種の処理を行う。

[0016] 端末20は、演算部21、記憶部22、通信部23、入力部24、表示部25等を備える。端末20の演算部21、記憶部22及び通信部23の機能的な特徴は、サーバ10の演算部11、記憶部12及び通信部13と同様である。入力部24は、例えばキーボード、マウス等を有し、端末20を操作する利用者からの入力操作を受け付ける。表示部25は、例えば液晶ディスプレイ等の表示装置、ビデオカード等を有し、端末20の演算部21による処理に応じた表示出力を行う。

[0017] 本実施形態の情報処理システムは、送信者に用いられる端末20である端末20aと受信者に用いられる端末20である端末20bとが別個の端末である。演算部21、記憶部22、通信部23、入力部24、表示部25の符号は、送信者の端末20aの演算部21a、記憶部22a、通信部23a、入力部24a、表示部25aと、受信者の端末20bの演算部21b、記憶部22b、通信部23b、入力部24b、表示部25bとを区別しない場合の符号である。情報処理システムは、暗号化対象情報54(p)の暗号化(以下、単に暗号化)又は暗号化後に送信される情報の復号化(以下、単に復号化)に係るデータを保持している。具体的には、例えば、サーバ10の記憶部12は、暗号化に用いられるマスター公開鍵51(G)及び受信者公開鍵53(s・G)を記憶している。送信者の端末20aは、暗号化対象情報54(p)の取り扱いに際して暗号化対象情報54(p)の暗号化に係る各種の処理を演算部21aに実行させるためのプログラム等である暗号化プログラム31を記憶している。受信者の端末20bは、暗号化対象情報54(p)の取り扱いに際して、暗号化プログラム31を用いて暗号化された暗号化対象情報54(p)の復号化に係る各種の処理を演算部21bに実行させるためのプログラム等である復号化プログラム32と、受信者公開鍵53(s・G)の作成及び復号化に用いられる受信者秘密鍵52(s)を記憶している。

[0018] なお、端末20は、1台であってもよい。その場合、情報処理システムは、例えば利用者毎の認証処理等、端末20を操作する者が送信者であるか受信者を識別する仕組みを有している。この他、図示しないが、サーバ10は、送信者と受信者との間での情報の送受信を仲介するサービス（例えば、電子メールの送受信サービス）を実行している。

[0019] 次に、暗号化及び復号化について説明する。マスター公開鍵51（G）は、楕円曲線上の座標（Gx, Gy）を示すデータである。楕円曲線を示す方程式は、例えば図4に示すものと同様、以下の式（2）のように表すことができる。式（2）におけるa、b、mは、それぞれ、xの係数、定数項、法である。

$$y^2 = x^3 + a \cdot x + b \pmod{m} \cdots (2)$$

[0020] 図5は、楕円曲線L1の一例を示す図である。楕円曲線L1上の特定の座標（例えば、座標P1）を基準とすると、当該座標を通る楕円曲線L1の接線と楕円曲線L1との交点の座標（例えば、座標Pt1）をy軸方向について反転した座標（例えば、座標P2）は、基準となる座標の2倍算を示す。すなわち、図5における座標P2は、座標P1の2倍算を示す。なお、2倍算は、同一座標同士の加算を示す。例えば、座標P2は、座標P1と座標P1との加算である。また、楕円曲線L1上の特定の2つの座標（例えば、座標P1, P2）を加算した座標は、当該2つの座標を結ぶ直線と楕円曲線L1との交点の座標（例えば、座標Pt2）をy軸方向について反転した座標（例えば、座標P3）である。すなわち、図5における座標P3は、座標P1と座標P2との加算を示す。ここで、座標P2は、座標P1の2倍算であるので、座標P1と座標P2との加算である座標P3は、座標P1の3倍算を示す。このように、楕円曲線L1上の座標における加算は、単に座標の数値を加算するものとは異なり、楕円曲線L1上の座標における乗算は、単に座標の数値を乗算するものとは異なることから、複雑になる。ただし、楕円曲線暗号を採用した場合の暗号化及び復号化に伴う係る複雑な演算は、コンピュータ上でバイナリ法等を用いることで効率的に行うことができる。

[0021] 座標 P_1 , P_2 , P_3 を用いて座標 P_1 の 4 倍算を求める方法は 2 つある。1 つは、座標 P_1 の 2 倍算である座標 P_2 の 2 倍算を求める方法である。もう 1 つは、座標 P_1 と、座標 P_1 の 3 倍算である座標 P_3 との加算を求める方法である。ここで、座標 P_2 を通る楕円曲線 L_1 の接線と楕円曲線 L_1 との交点の座標 (座標 P_{t3}) を y 軸方向について反転した座標 (座標 P_4) と、座標 P_1 と座標 P_3 とを結ぶ直線と楕円曲線 L_1 との交点の座標 (座標 P_{t3}) を y 軸方向について反転した座標 (例えば、座標 P_4) とは一致する。これは、座標 P_4 のような N 倍算を効率的に求める方法が複数あり、より効率的な方法で N 倍算を行うことができることを示唆する。

[0022] 図 5 を参照して説明した楕円曲線 L_1 の性質は、楕円曲線 L_1 上の座標 P_1 のスカラー (例えば、スカラー D) 倍算である $D \times P_1$ (例えば、 $D = 4$ である場合、 $D \times P_1 = P_4$) を求めることが容易であることを示す。一方、座標 P_1 と、座標 P_1 のスカラー倍算である座標 (例えば、座標 P_4) からスカラー (D) を求めることは、楕円曲線 L_1 上の離散対数問題の観点から困難である。この容易さと困難さの非対称性は、楕円曲線暗号の安全性、すなわち暗号化された情報の秘匿性 (暗号強度) の高さを示している。

[0023] また、楕円曲線暗号は、RSA 暗号と比較した場合、同レベルの安全性をより短い鍵で実現できる。例えば、RSA 暗号において 1024 ビットの暗号鍵を用いた場合と、楕円曲線暗号で 160 ビットの暗号鍵を用いた場合の暗号強度はほぼ等しいとされている。これは、楕円曲線暗号は、RSA 暗号に比して処理負荷がより小さく、同レベルの安全性を確保する目的であれば処理速度がより早くなることを示している。

[0024] 上記で説明した理由により、本発明は、楕円曲線暗号を採用しており、マスター公開鍵 51 (G) として、楕円曲線 L_1 上の座標 (G_x , G_y) を示すデータを用いている。係る座標 (G_x , G_y) は、二次元の情報を示すデータであると捉えることができる。マスター公開鍵 51 (G) は、サーバ 10 によって公開状態で保持されており、マスター公開鍵 51 (G) が示す座標を端末 20 から把握可能になっている。

[0025] 受信者秘密鍵 5 2 (s) は、スカラー形式のデータである。スカラー形式のデータは、一次元の情報を示すデータであると捉えることができ、数値に置換可能である。受信者公開鍵 5 3 ($s \cdot G$) は、マスター公開鍵 5 1 (G) が示す座標 (G_x , G_y) に受信者秘密鍵 5 2 (s) を乗じたスカラー倍算である。受信者秘密鍵 5 2 (s) は、例えば受信者の端末 2 0 b に非公開状態で設定、保持されている。すなわち、受信者秘密鍵 5 2 (s) は、受信者のみが知りうるデータである。受信者は、予め任意の受信者秘密鍵 5 2 (s) を設定することができる。受信者公開鍵 5 3 ($s \cdot G$) は、設定された受信者秘密鍵 5 2 (s) とサーバ 1 0 で公開されているマスター公開鍵 5 1 (G) とを用いて演算により生成され、サーバ 1 0 に公開状態で保持される。受信者は、手動で受信者公開鍵 5 3 ($s \cdot G$) を生成してサーバ 1 0 に公開することができる。上記で説明した楕円曲線暗号の安全性に基づき、マスター公開鍵 5 1 (G) が示す座標 (G_x , G_y) に受信者秘密鍵 5 2 (s) を乗じたスカラー倍算の算出は容易である一方、マスター公開鍵 5 1 (G) と受信者公開鍵 5 3 ($s \cdot G$) から受信者秘密鍵 5 2 (s) を特定することは困難である。

[0026] 受信者秘密鍵 5 2 (s) は、情報処理システムによって自動的に設定されてもよい。具体的には、例えば、受信者の端末 2 0 b の記憶部 2 2 b に記憶されている復号化プログラム 3 2 を実行処理した演算部 2 1 b による機能の 1 つとして、受信者秘密鍵 5 2 (s) を自動的に設定する機能を設けてもよい。同様に、受信者公開鍵 5 3 ($s \cdot G$) は、情報処理システムによって自動的に設定されてもよい。

[0027] 暗号化対象情報 5 4 (p) は、送信者から受信者宛てに送信される非公開情報である。暗号化対象情報 5 4 (p) とするデータは任意であるが、例えば送信者から受信者に伝達したいパスワード等の文字列である。暗号化対象情報 5 4 (p) は、暗号化して送信したいドキュメントデータ、画像データ、音声データ等であってもよいし、これらのデータのいずれか又は複数を圧縮した圧縮データであってもよい。どのようなデータであっても、デジタル

データは所定のルールに基づいてスカラーに置換可能であるので、暗号化対象情報 54 (p) とすることができる。図 4 では、送信者の端末 20 a で暗号化される前の暗号化対象情報 54 (p) に符号 54 a を付し、受信者の端末 20 b で復号化された第 3 復号化情報である暗号化対象情報 54 (p) に符号 54 b を付している。暗号化対象情報 54 a, 54 b は同一のデータである。以下、符号 54 a, 54 b を用いて暗号化前の暗号化対象情報 (p) と復号化後の暗号化対象情報 (p) とを区別することがある。

[0028] 乱数 56 (r) は、予め設定される所定のスカラー（例えば、数値）である。乱数 56 (r) は、例えば送信者の端末 20 a で演算部 21 a が暗号化プログラム 31 を実行処理することで自動的に設定される値であるが、これは乱数 56 (r) の設定方法の一例であって適宜変更可能である。例えば、送信者が任意の乱数 56 (r) を手動で設定してもよい。

[0029] 中間鍵 55 (P) は、マスター公開鍵 51 (G) が示す座標 (G_x, G_y) に暗号化対象情報 54 a (p) を乗じたスカラー倍算 ($p \cdot G$) である。中間鍵 55 (P) が示す座標 (P_x, P_y) は、座標 ($(p \cdot G)_x, (p \cdot G)_y$) である。暗号化対象情報 54 a (p)、乱数 56 (r) 及び中間鍵 55 (P) は、送信者の端末 20 a に非公開状態で取り扱われる。すなわち、送信者の端末 20 a で取り扱われている暗号化対象情報 54 a (p)、乱数 56 (r) 及び中間鍵 55 (P) は、送信者のみが知りうるデータである。ただし、中間鍵 55 (P) は、暗号化対象情報 54 (p) の復号化に係る処理において受信者の端末 20 b で復号化される。図 4 では、送信者の端末 20 a で取り扱われる中間鍵 55 (P) に符号 55 a を付し、受信者の端末 20 b で復号化された第 2 復号化情報である中間鍵 55 (P) に符号 55 b を付している。以下、符号 55 a, 55 b を用いて中間鍵 55 (P) を区別することがある。中間鍵 55 a, 55 b は同一のデータである。

[0030] 第 1 送信情報 57 (C1) は、マスター公開鍵 51 (G) が示す座標 (G_x, G_y) に乱数 56 (r) を乗じたスカラー倍算 ($r \cdot G$) である。第 1 送信情報 57 (C1) が示す座標 ($C1_x, C1_y$) は、座標 ($(r \cdot G)$

$x, (r \cdot G) y$ である。第2送信情報58 (C2) は、中間鍵55a (P) と、受信者公開鍵53 ($s \cdot G$) に乱数56 (r) を乗じたスカラー倍算 ($r \cdot (s \cdot G)$) とを加算したデータ ($P + r \cdot (s \cdot G)$) である。第2送信情報58 (C2) が示す座標 ($C2x, C2y$) は、座標 ($(P + r \cdot (s \cdot G)) x, (P + r \cdot (s \cdot G)) y$) である。第3送信情報59 (c3) は、暗号化対象情報54a (p) と、中間鍵55a (P) のx座標 (Px) とを加算したデータ ($p + Px$) である。ここで、中間鍵55a (P) の座標 (Px, Py) は二次元の座標を示すが、x座標 (Px) は一次元の情報であるので、第3送信情報59 (c3) は、一次元のデータである。

[0031] 第3送信情報59 (c3) は、暗号化対象情報54a (p) を暗号化した情報として機能する。第1送信情報57 (C1) 及び第2送信情報58 (C2) は、第3送信情報59 (c3) から暗号化対象情報54 (p) を復号化するための情報として機能する。第1送信情報57 (C1)、第2送信情報58 (C2) 及び第3送信情報59 (c3) は、送信者から受信者に送信される。すなわち、第1送信情報57 (C1)、第2送信情報58 (C2) 及び第3送信情報59 (c3) は、通信回線Nを経由して送信者の端末20aの外部に伝送 (公開) される。このため、通信回線N等に対して第三者が介入することで第1送信情報57 (C1)、第2送信情報58 (C2) 及び第3送信情報59 (c3) が第三者に取得される可能性はゼロでない。しかしながら、暗号化対象情報54 (p) が第3送信情報59 (c3) として暗号化されているため、第三者は、暗号化対象情報54 (p) の内容を把握することができない。

[0032] 第1復号用情報60 ($s \cdot C1$) は、第1送信情報57 (C1) が示す座標 ($C1x, C1y$) に受信者秘密鍵52 (s) を乗じたスカラー倍算 ($s \cdot (r \cdot G)$) である。第1送信情報57 (C1) が示す座標 ($s \cdot C1x, s \cdot C1y$) は、座標 ($(s \cdot (r \cdot G)) x, (s \cdot (r \cdot G)) y$) である。ここで、 $s \cdot (r \cdot G)$ と $r \cdot (s \cdot G)$ は、双方ともマスター公

開鍵 5 1 (G) にスカラー (r) 及びスカラー (s) を乗じたスカラー倍算であり、同値である。第 1 復号用情報 6 0 ($s \cdot C 1$) と第 2 送信情報 5 8 (C 2) とに基づいて、中間鍵 5 5 b (P) を得ることができる。具体的には、以下の式 (3) によって中間鍵 5 5 b (P) を導出することができる。すなわち、第 2 送信情報 5 8 (C 2) で中間鍵 5 5 a (P) に加算されているスカラー倍算 (乱数 5 6 (r) と受信者公開鍵 5 3 ($s \cdot G$) との乗算である $r \cdot (s \cdot G)$) と、第 1 復号用情報 6 0 ($s \cdot C 1$) であるスカラー倍算 ($s \cdot (r \cdot G)$) とは同値であることから、第 2 送信情報 5 8 (C 2) から第 1 復号用情報 6 0 ($s \cdot C 1$) を差し引くことで、中間鍵 5 5 b (P) を復号することができることになる。復号された中間鍵 5 5 b (P) から、座標 (P_x , P_y) を特定することができる。

$$\begin{aligned} P &= C 2 - s \cdot C 1 \\ &= (P + r \cdot (s \cdot G)) - s \cdot (r \cdot G) \\ &= P + r \cdot (s \cdot G) - r \cdot (s \cdot G) \cdots (3) \end{aligned}$$

[0033] 中間鍵 5 5 b (P) の座標 (P_x) と第 3 送信情報 5 9 (c 3) とに基づいて、暗号化対象情報 5 4 b (p) を得ることができる。具体的には、以下の式 (4) によって暗号化対象情報 5 4 b (p) を導出することができる。すなわち、第 1 復号用情報 6 0 ($s \cdot C 1$) と第 2 送信情報 5 8 (C 2) とに基づいて復号化された中間鍵 5 5 b (P) と第 3 送信情報 5 9 (c 3) から暗号化対象情報 5 4 b (p) を復号することができることになる。第 1 復号用情報 6 0 ($s \cdot C 1$) は第 1 送信情報 5 7 (C 1) と受信者秘密鍵 5 2 (s) から得られているので、第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (c 3) 並びに受信者秘密鍵 5 2 (s) から暗号化対象情報 5 4 b (p) を復号することができる。第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (c 3) は、送信者から受信者に送信されている。受信者秘密鍵 5 2 (s) は、受信者側で保持されている情報である。従って、受信者は、送信者から送信された第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (

c 3) と、既知の受信者秘密鍵 5 2 (s) とに基づいて、暗号化対象情報 5 4 b (p) を復号することができる。

$$\begin{aligned} p &= c 3 - P x \\ &= (p + P x) - P x \cdots (4) \end{aligned}$$

[0034] 図 6～図 8 のフローチャートを参照して、情報処理システムによる暗号化及び復号化に係る処理の流れの一例を説明する。図 6 は、受信者による準備処理の流れの一例を示すフローチャートである。受信者の端末 2 0 b の演算部 2 1 b は、記憶部 2 2 b から復号化プログラム 3 2 を読み出して実行処理し、受信者公開鍵 5 3 (s · G) の公開に係る各種の処理を行う。具体的には、演算部 2 1 b は、通信部 2 3 b を介して、サーバ 1 0 からマスター公開鍵 5 1 (G) を取得する (ステップ S 1)。また、演算部 2 1 b は、受信者秘密鍵 5 2 (s) を設定する (ステップ S 2)。ステップ S 1 の処理とステップ S 2 の処理は、順不同である。演算部 2 1 b は、受信者秘密鍵 5 2 (s) とマスター公開鍵 5 1 (G) から受信者公開鍵 5 3 (s · G) を生成する (ステップ S 3)。演算部 2 1 b は、通信部 2 3 b を介して、受信者公開鍵 5 3 (s · G) をサーバ 1 0 に送信して公開する (ステップ S 4)。これらの処理に係る機能は、例えば、復号化プログラム 3 2 の一機能として実装されていてもよいし、専用のプログラムとして設けられていてもよい。また、これらの処理は、受信者による手動の入力操作に応じて行われてもよい。

[0035] 図 7 は、送信者による暗号化処理及びデータの送信に係る処理の流れの一例を示すフローチャートである。送信者の端末 2 0 a の演算部 2 1 a は、記憶部 2 2 a から暗号化プログラム 3 1 を読み出して実行処理し、暗号化対象情報 5 4 a (p) の暗号化及び暗号化後のデータの送信に係る各種の処理を行う。具体的には、演算部 2 1 a は、例えば、サーバ 1 0 からマスター公開鍵 5 1 (G) 及び受信者公開鍵 5 3 (s · G) を取得する (ステップ S 1 1)。演算部 2 1 a は、暗号化対象情報 5 4 a (p) を設定する (ステップ S 1 2)。演算部 2 1 a は、暗号化対象情報 5 4 a (p) とマスター公開鍵 5 1 (G) から中間鍵 5 5 a (P) を生成する (ステップ S 1 3)。演算部 2

1 a は、乱数 5 6 (r) を設定する (ステップ S 1 4)。演算部 2 1 a は、乱数 5 6 (r) とマスター公開鍵 5 1 (G) から第 1 送信情報 5 7 (C 1) を生成する (ステップ S 1 5)。演算部 2 1 a は、中間鍵 5 5 a (P) と乱数 5 6 (r) と受信者公開鍵 5 3 (s · G) から第 2 送信情報 5 8 (C 2) を生成する (ステップ S 1 6)。演算部 2 1 a は、暗号化対象情報 5 4 a (p) と中間鍵 5 5 a (P) から第 3 送信情報 5 9 (c 3) を生成する (ステップ S 1 7)。演算部 2 1 a は、なお、ステップ S 1 2 の処理は、例えば、受信者の端末 2 0 b において受信者が手動で暗号化対象情報 5 4 a (p) とするデータを選択決定又は生成することで行われる。ステップ S 1 1 の処理、ステップ S 1 2 の処理、ステップ S 1 4 の処理は、順不同である。ステップ S 1 3 の処理、ステップ S 1 4 の処理は、順不同である。ステップ S 1 5 の処理、ステップ S 1 6 の処理、ステップ S 1 7 の処理は、順不同である。

[0036] 送信者の端末 2 0 a の演算部 2 1 a は、通信部 2 3 a を介して、第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (c 3) を受信者に送信するためのデータの送信を行う (ステップ S 1 8)。本実施形態では、演算部 2 1 a は、例えば電子メールの添付ファイルとして第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (c 3) をサーバ 1 0 に送信する。係る電子メールの宛先となるメールアドレスは、受信者のメールアドレスである。サーバ 1 0 は、送信者の端末 2 0 a から送信された第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (c 3) を受信者の端末 2 0 b に送信する。

[0037] 図 8 は、受信者による復号化処理の流れの一例を示すフローチャートである。受信者の端末 2 0 b の演算部 2 1 b は、記憶部 2 2 b から復号化プログラム 3 2 及び受信者秘密鍵 5 2 (s) を読み出して実行処理し、第 3 送信情報 5 9 (c 3) からの暗号化対象情報 5 4 b (p) の復号化に係る各種の処理を行う。具体的には、演算部 2 1 b は、通信部 2 3 b を介して、第 1 送信情報 5 7 (C 1)、第 2 送信情報 5 8 (C 2) 及び第 3 送信情報 5 9 (c 3) を受信する (ステップ S 2 1)。演算部 2 1 b は、第 1 送信情報 5 7 (C

1) と受信者秘密鍵 52 (s) から第1復号用情報 60 ($s \cdot C1$) を生成する(ステップ S22)。演算部 21b は、第2送信情報 58 (C2) と第1復号用情報 60 ($s \cdot C1$) から中間鍵 55b (P) を復号する(ステップ S23)。演算部 21b は、復号された中間鍵 55b (P) と第3送信情報 59 (c3) から暗号化対象情報 54b (p) を復号する(ステップ S24)。

[0038] このように、本実施形態では、非公開情報である暗号化対象情報 54 (p) の取り扱いに際して、楕円曲線上の座標を示す公開情報であるマスター公開鍵 51 (G) の設定工程と、非公開情報である受信者秘密鍵 52 (s) とマスター公開鍵 51 (G) との積を示す公開情報である受信者公開鍵 53 ($s \cdot G$) を生成する工程と、非公開情報である暗号化対象情報 54a (p) とマスター公開鍵 51 (G) との積を示す非公開情報である中間鍵 55a ($P = p \cdot G$) を生成する工程と、非公開情報である乱数 56 (r) とマスター公開鍵 51 (G) との積を示す第1送信情報 57 ($C1 = r \cdot G$) を生成する工程と、乱数 56 (r) と受信者公開鍵 53 ($s \cdot G$) との積と、中間鍵 55a (P) との加算を示す第2送信情報 58 ($C2 = P + r \cdot (s \cdot G)$) を生成する工程と、少なくとも暗号化対象情報 54a (p) 及び中間鍵 55a (P) が示す情報を用いた演算によって導出される第3送信情報 59 ($c3 = p + P \times$) を生成する工程と、受信者秘密鍵 52 (s) と第1送信情報 57 (C1) との積である第1復号用情報 60 ($s \cdot C1 = s \cdot (r \cdot G) = r (s \cdot G)$) を生成する工程と、第2送信情報 58 (C2) から第1復号用情報 60 ($s \cdot C1$) を減じて中間鍵 55b (P) を得る工程 ($P = C2 - s \cdot C1 = P + r \cdot (s \cdot G) - r \cdot (s \cdot G)$) と、中間鍵 55b (P) と第3送信情報 59 (c3) に基づいて暗号化対象情報 54b (p) を得る工程 ($p = c3 - P \times = p + P \times - P \times$) と、を有する情報処理方法が実施されている。

[0039] また、本実施形態の情報処理システムは、情報の送信者及び情報の受信者が操作する1つ以上の端末 20 と、端末 20 と通信可能に接続されたサーバ

10とを有し、送信者から受信者宛てに送信される非公開情報である暗号化対象情報54を暗号化する情報処理システムであって、サーバ10は、楕円曲線上の座標を示す公開情報であるマスター公開鍵51及び非公開情報である受信者秘密鍵52とマスター公開鍵51との積を示す公開情報である受信者公開鍵53を記憶する第1記憶部（記憶部12）を備え、端末20又はサーバ10は、暗号化対象情報54aとマスター公開鍵51との積を示す非公開情報である中間鍵55aを生成する中間鍵生成部と、非公開情報である乱数56とマスター公開鍵51との積を示す第1送信情報57、乱数56と受信者公開鍵53との積と中間鍵55aとの加算を示す第2送信情報58、少なくとも暗号化対象情報54a及び中間鍵55aが示す情報を用いた演算によって導出される第3送信情報59を生成する暗号化部と、受信者秘密鍵52と第1送信情報57との積である第1復号用情報60を算出し、第2送信情報58から第1復号用情報を減じて中間鍵55bを導出し、導出された中間鍵55bと第3送信情報59に基づいて暗号化対象情報54bを得る復号化部と、を備える情報処理システムである。

[0040] 具体的には、送信者の端末20aの演算部21aは、暗号化プログラム31を実行することで、暗号化対象情報54aとマスター公開鍵51との積を示す非公開情報である中間鍵55aを生成する中間鍵生成部として機能する。また、送信者の端末20aの演算部21aは、暗号化プログラム31を実行することで、非公開情報である乱数56とマスター公開鍵51との積を示す第1送信情報57、乱数56と受信者公開鍵53との積と中間鍵55aとの加算を示す第2送信情報58、少なくとも暗号化対象情報54a及び中間鍵55aが示す情報を用いた演算によって導出される第3送信情報59を生成する暗号化部として機能する。また、受信者の端末20bの演算部21bは、復号化プログラム32を実行することで、受信者秘密鍵52と第1送信情報57との積である第1復号用情報60を算出し、第2送信情報58から第1復号用情報60を減じて中間鍵55bを導出し、導出された中間鍵55bと第3送信情報59に基づいて暗号化対象情報54bを得る復号化部とし

て機能する。

[0041] また、本実施形態の情報処理システムにおいて、送信者の端末20aは、中間鍵生成部及び暗号化部を備え、受信者の端末20bは、復号化部と、受信者秘密鍵52を記憶する第2記憶部（記憶部22）とを備え、送信者の端末20aは、第1送信情報57、第2送信情報58及び第3送信情報59をサーバ10に送信し、サーバ10は、第1送信情報57、第2送信情報58及び第3送信情報59を受信者の端末20bに送信する。

[0042] 以上、本実施形態によれば、中間鍵55a（ $P : p \cdot G$ ）を生成し、中間鍵55a（ P ）が示す情報を用いた演算によって導出される第2送信情報58（ $C2 : P + r \cdot (s \cdot G)$ ）及び第3送信情報59（ $c3 : p + P \cdot x$ ）を生成するので、暗号化対象情報54（ p ）を得るための具体的な処理内容の特定をより困難にすることができる。よって、より高い機密性を確保することができる。

[0043] また、第3送信情報59は、中間鍵55a（ P ）が示す x 座標と暗号化対象情報54a（ p ）との加算（ $c3 : p + P \cdot x$ ）であるので、簡単な演算で暗号化対象情報54a（ p ）を暗号化することができ、より低い処理負荷でより高い機密性を確保することができる。

[0044] また、端末20が暗号化及び復号化に係る処理を行うので、暗号化対象情報54（ p ）の取り扱いにおけるサーバ10の負荷を最小限にすることができる。

[0045] 特に、暗号化対象情報を共通鍵方式で用いられるパスワードにすることで、共通鍵方式を利用した暗号化を伴うデータの伝送に際して受信者に伝えられるパスワードの機密性を確保することができる。このように、送信者が任意に設定するパスワード等の伝達に係る第三者の介入の可能性を効果的に抑制する仕組みを高い利便性で提供することができる。また、パーソナルコンピュータ（PC）等の情報処理装置に搭載されているTPM（Trusted Platform Module）等のセキュリティチップで取り扱われる公開鍵を本発明の公開鍵とすることで、公開鍵を自動的に生成及び公開することができるように

なる。よって、受信者の立場になりうるユーザは、受信者秘密鍵 5 2 (s) を設定するだけで受信者公開鍵 5 3 (s · G) を公開することができるようになる。よって、より簡便に、送信者から暗号化対象情報 5 4 (p) として送られる 1 次元の情報（例えば、パスワード等）を暗号化された状態で受信し、受信者のみが復号することができるようになり、利便性が飛躍的に向上する。

[0046] (変形例)

なお、第 3 送信情報 5 9 (c 3) は上記の実施形態で例示した情報 (p + P x) に限られず、適宜変更可能である。例えば、中間鍵 5 5 a (P) が示す x 座標 (P x) に代えて、中間鍵 5 5 a (P) が示す y 座標 (P y) を暗号化対象情報 5 4 a (p) に加算した情報を第 3 送信情報 (c 3) としてもよい。

[0047] また、第 3 送信情報 (c 3) は、第 1 送信情報 5 7 (C 1) が示す x 座標 (C 1 x) と中間鍵 5 5 a (P) が示す x 座標 (P x) との積と、第 1 送信情報 5 7 (C 1) が示す y 座標 (C 1 y) と中間鍵 5 5 a (P) が示す y 座標 (P y) との積とが暗号化対象情報 5 4 (p) に付加された情報であってもよい。すなわち、以下の式 (5) が成立するようにしてもよい。この場合、第 1 送信情報 5 7 (C 1) から、第 1 送信情報 5 7 (C 1) が示す x 座標 (C 1 x) 及び y 座標 (C 1 y) が得られる。また、第 2 送信情報 5 8 (C 2) から第 1 復号用情報 6 0 (s · C 1) を減じて得た中間鍵 5 5 b (P) から、中間鍵 5 5 b (P) が示す x 座標 (P x) 及び y 座標 (P y) が得られる。よって、このようにして得られた第 1 送信情報 5 7 (C 1) が示す x 座標 (C 1 x) と中間鍵 5 5 b (P) が示す x 座標 (P x) の乗算 (C 1 x × P x) と、第 1 送信情報 5 7 (C 1) が示す y 座標 (C 1 y) と中間鍵 5 5 b (P) が示す y 座標 (P y) の乗算 (C 1 y × P y) とを第 3 送信情報 (c 3) から減ずることで、暗号化対象情報 5 4 b (p) を復号することができる。

$$c\ 3 = p + (C\ 1\ x \times P\ x) + (C\ 1\ y \times P\ y) \cdots (5)$$

[0048] また、中間鍵 5 5 a (P) が示す x 座標 (P_x)、中間鍵 5 5 a (P) が示す y 座標 (P_y)、第 1 送信情報 5 7 (C 1) が示す x 座標 (C_{1x})、第 1 送信情報 5 7 (C 1) が示す y 座標 (C_{1y})、第 2 送信情報 5 8 (C 2) が示す x 座標 (C_{2x})、第 2 送信情報 5 8 (C 2) が示す y 座標 (C_{2y})、第 3 送信情報 (c 3) に基づいて、式 (1) が成立するようにしてもよい。この場合、第 1 送信情報 5 7 (C 1) から、第 1 送信情報 5 7 (C 1) が示す x 座標 (C_{1x}) 及び y 座標 (C_{1y}) が得られる。また、第 2 送信情報 5 8 (C 2) から第 1 復号用情報 6 0 ($s \cdot C_1$) を減じて得た中間鍵 5 5 b (P) から、中間鍵 5 5 b (P) が示す x 座標 (P_x) 及び y 座標 (P_y) が得られる。よって、これらを用いて、第 1 送信情報 5 7 (C 1) が示す x 座標 (C_{1x}) を底として中間鍵 5 5 b (P) が示す x 座標 (P_x) を冪指数とする第 1 冪演算値 ($C_{1x}^{P_x}$) 及び第 1 送信情報 5 7 (C 1) が示す y 座標 (C_{1y}) を底として中間鍵 5 5 b (P) が示す y 座標 (P_y) を冪指数とする第 2 冪演算値 ($C_{1y}^{P_y}$) が得られる。また、第 2 送信情報 5 8 (C 2) から、第 2 送信情報 5 8 (C 2) が示す x 座標 (C_{2x}) 及び y 座標 (C_{2y}) が得られる。よって、これらを用いて、第 1 冪演算値 ($C_{1x}^{P_x}$) を第 2 送信情報 5 8 (C 2) が示す x 座標 (C_{2x}) で割った剰余 ($C_{1x}^{P_x} \bmod C_{2x}$) と第 2 冪演算値 ($C_{1y}^{P_y}$) を第 2 送信情報 5 8 (C 2) が示す y 座標 (C_{2y}) で割った剰余 ($C_{1y}^{P_y} \bmod C_{2y}$) を求め、第 3 送信情報 (c 3) から減ずることで、暗号化対象情報 5 4 b (p) を復号することができる。

$$c_3 = (C_{1x}^{P_x} \bmod C_{2x}) + (C_{1y}^{P_y} \bmod C_{2y}) + p \cdots (1)$$

[0049] このように第 3 送信情報 (c 3) を適宜変更することで、第 3 送信情報 (c 3) から暗号化対象情報 5 4 を得るための具体的な処理内容の特定をより困難にすることができる。よって、より高い機密性を確保することができる。

[0050] 上記の実施形態及び変形例はあくまで一例であり、本発明の技術的特徴を

逸脱しない範囲内において適宜変更可能である。例えば、暗号化プログラム 3 1 及び復号化プログラム 3 2 が提供している機能の一部又は全部をサーバ 1 0 で実行処理する所謂サーバクライアントモデルで暗号化及び復号化を行うようにしてもよい。

符号の説明

[0051]	1 0	サーバ
	1 1	演算部
	1 2	記憶部
	1 3	通信部
	2 0, 2 0 a, 2 0 b	端末
	2 1, 2 1 a, 2 1 b	演算部
	2 2, 2 2 a, 2 2 b	記憶部
	2 3, 2 3 a, 2 3 b	通信部
	2 4, 2 4 a, 2 4 b	入力部
	2 5, 2 5 a, 2 5 b	表示部
	3 1	暗号化プログラム
	3 2	復号化プログラム
	5 1	マスター公開鍵
	5 2	受信者秘密鍵
	5 3	受信者公開鍵
	5 4, 5 4 a, 5 4 b	暗号化対象情報
	5 5, 5 5 a, 5 5 b	中間鍵
	5 6	乱数
	5 7	第 1 送信情報
	5 8	第 2 送信情報
	5 9	第 3 送信情報
	6 0	第 1 復号用情報
	N	通信回線

請求の範囲

- [請求項1] 非公開情報である暗号化対象情報を取り扱う情報処理装置による情報処理方法であって、
- 楕円曲線上の座標を示す公開情報であるマスター公開鍵の設定工程と、
- 非公開情報である受信者秘密鍵と前記マスター公開鍵との積を示す公開情報である受信者公開鍵を生成する工程と、
- 非公開情報である暗号化対象情報と前記マスター公開鍵との積を示す非公開情報である中間鍵を生成する工程と、
- 非公開情報である乱数と前記マスター公開鍵との積を示す第1送信情報を生成する工程と、
- 前記乱数と前記受信者公開鍵との積と、前記中間鍵との加算を示す第2送信情報を生成する工程と、
- 少なくとも暗号化対象情報及び前記中間鍵が示す情報を用いた演算によって導出される第3送信情報を生成する工程と、
- 前記受信者秘密鍵と前記第1送信情報との積である第1復号用情報を生成する工程と、
- 前記第2送信情報から前記第1復号用情報を減じて前記中間鍵を得る工程と、
- 前記中間鍵と前記第3送信情報に基づいて前記暗号化対象情報を得る工程と
- を有する情報処理方法。
- [請求項2] 前記第3送信情報は、前記中間鍵が示す x 座標と前記暗号化対象情報との加算である
- 請求項1に記載の情報処理方法。
- [請求項3] 前記第3送信情報は、前記第1送信情報が示す x 座標と前記中間鍵が示す x 座標との積と、前記第1送信情報が示す y 座標と前記中間鍵が示す y 座標との積とが前記暗号化対象情報に付加された情報である

請求項 1 に記載の情報処理方法。

[請求項4]

前記中間鍵が示す x 座標を P_x とし、前記中間鍵が示す y 座標を P_y とし、前記第 1 送信情報が示す x 座標を $C_1 x$ とし、前記第 1 送信情報が示す y 座標を $C_1 y$ とし、前記第 2 送信情報が示す x 座標を $C_2 x$ とし、前記第 2 送信情報が示す y 座標を $C_2 y$ とし、前記第 3 送信情報を c_3 とし、前記暗号化対象情報を p とすると、式 (1) が成立する

請求項 1 に記載の情報処理方法。

$$c_3 = (C_1 x^{P_x} \bmod C_2 x) + (C_1 y^{P_y} \bmod C_2 y) + p \cdots (1)$$

[請求項5]

情報の送信者及び情報の受信者が操作する 1 つ以上の端末と、前記端末と通信可能に接続されたサーバとを有し、前記送信者から前記受信者宛てに送信される非公開情報である暗号化対象情報を暗号化する情報処理システムであって、

前記サーバは、

楕円曲線上の座標を示す公開情報であるマスター公開鍵及び非公開情報である受信者秘密鍵と前記マスター公開鍵との積を示す公開情報である受信者公開鍵を記憶する第 1 記憶部を備え、

前記端末又は前記サーバは、

前記暗号化対象情報と前記マスター公開鍵との積を示す非公開情報である中間鍵を生成する中間鍵生成部と、

非公開情報である乱数と前記マスター公開鍵との積を示す第 1 送信情報、前記乱数と前記受信者公開鍵との積と前記中間鍵との加算を示す第 2 送信情報、少なくとも暗号化対象情報及び前記中間鍵が示す情報を用いた演算によって導出される第 3 送信情報を生成する暗号化部と、

前記受信者秘密鍵と前記第 1 送信情報との積である第 1 復号用情報を算出し、前記第 2 送信情報から前記第 1 復号用情報を減じて前記中

間鍵を導出し、導出された前記中間鍵と前記第3送信情報に基づいて
前記暗号化対象情報を得る復号化部と

を備える情報処理システム。

[請求項6]

前記送信者の端末は、前記中間鍵生成部及び前記暗号化部を備え、
前記受信者の端末は、

前記復号化部と、

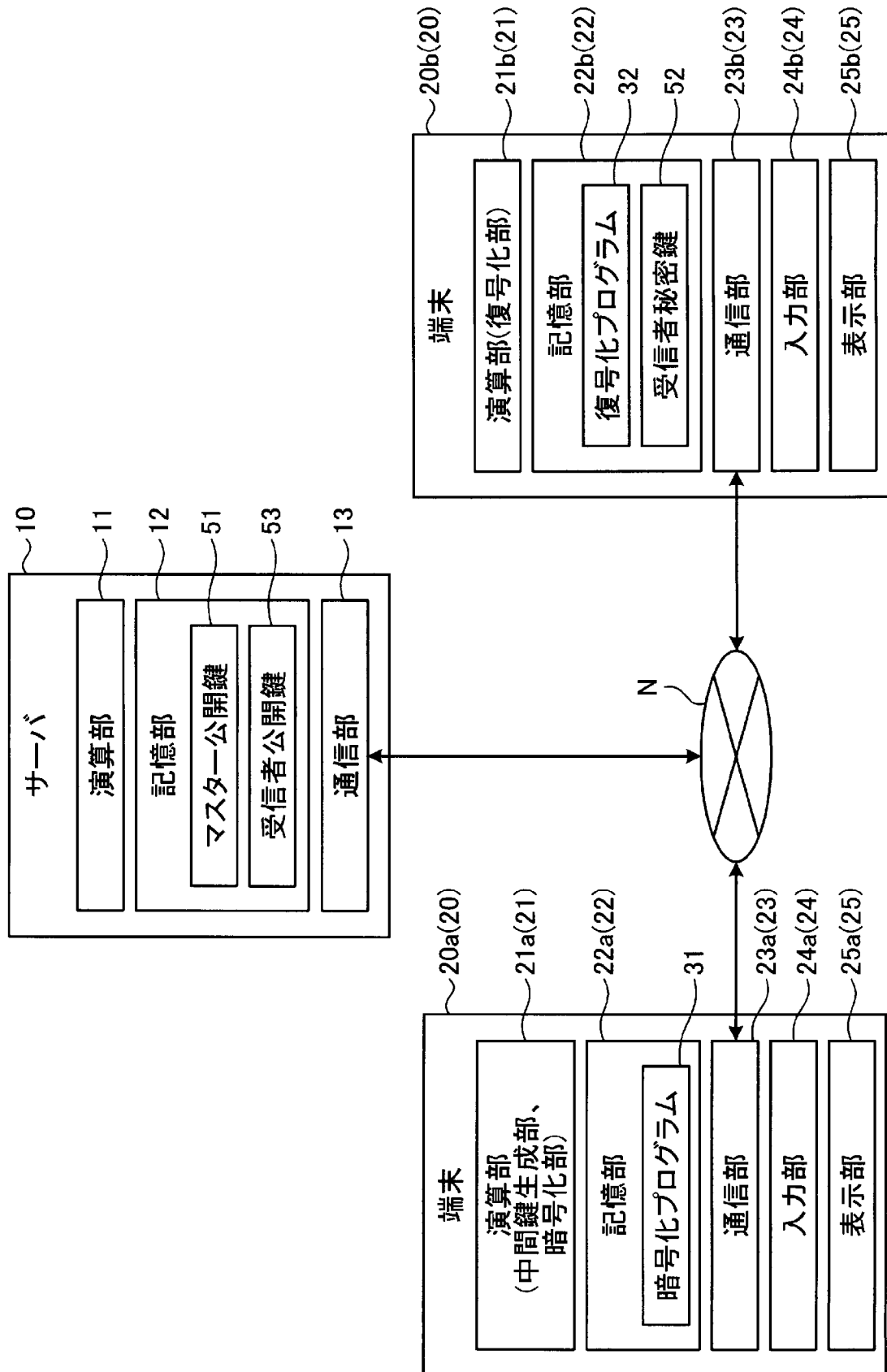
前記受信者秘密鍵を記憶する第2記憶部とを備え、

前記送信者の端末は、前記第1送信情報、前記第2送信情報及び前
記第3送信情報を前記サーバに送信し、

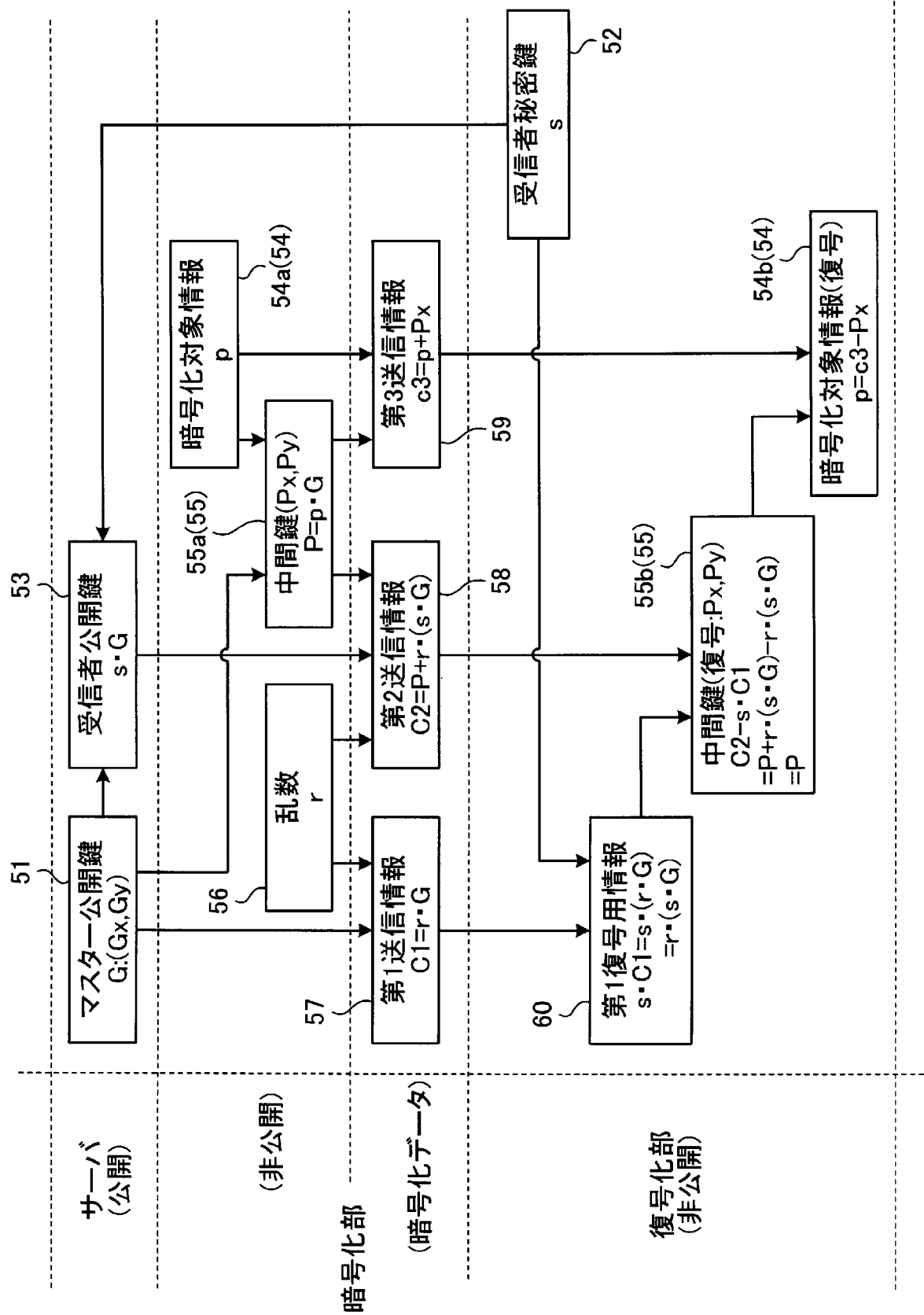
前記サーバは、前記第1送信情報、前記第2送信情報及び前記第3
送信情報を前記受信者の端末に送信する

請求項5に記載の情報処理システム。

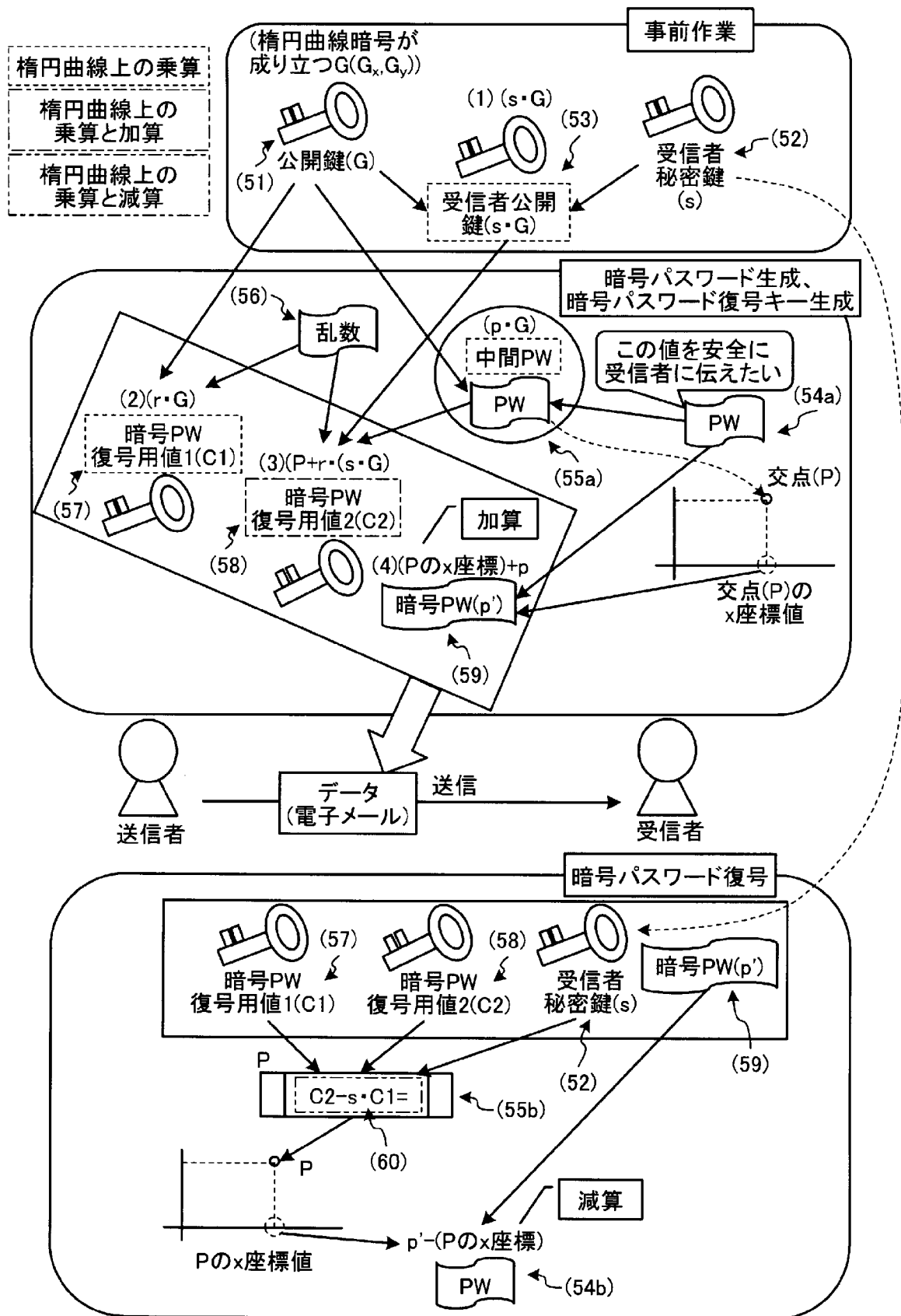
[図1]



[図2]



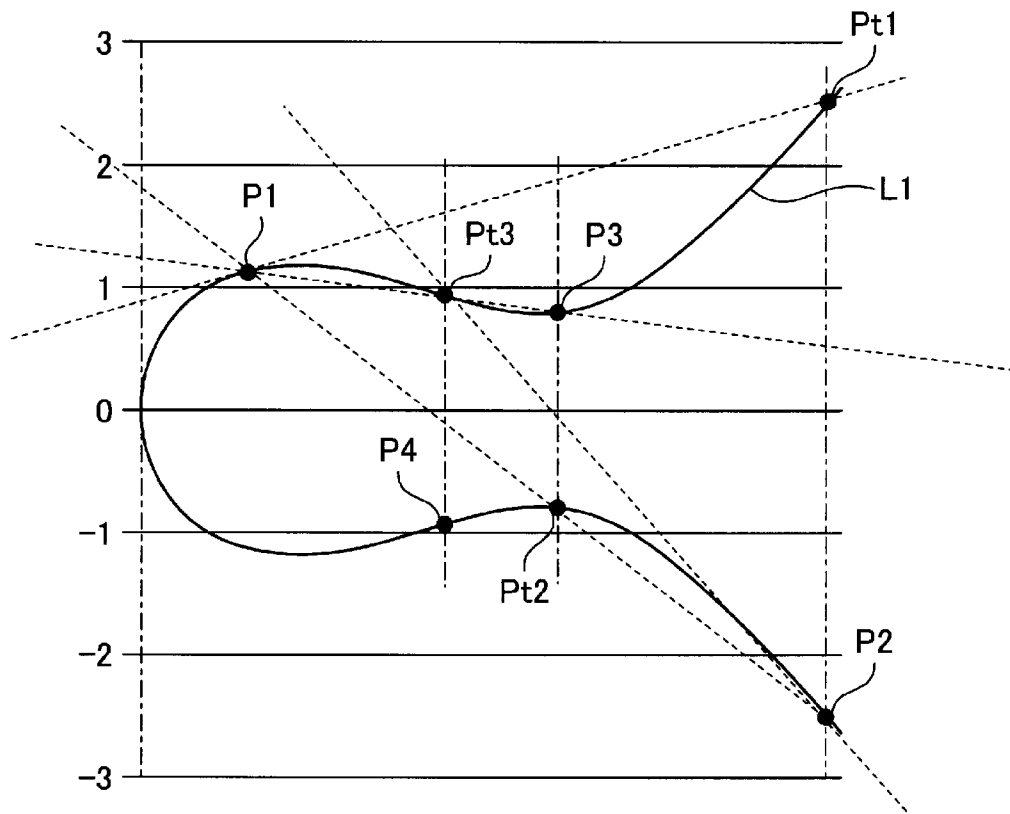
[図3]



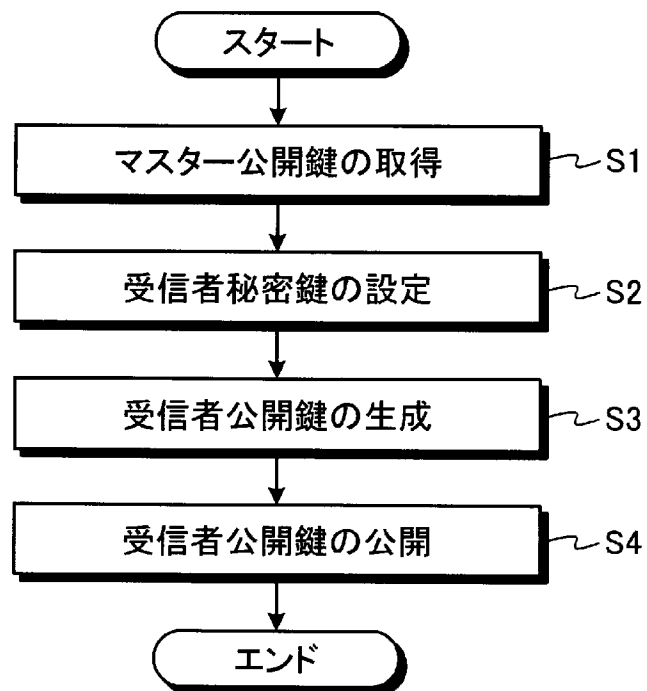
[図4]

既存 設定	楕円曲線	数式				公開
		$y^2=x^3+a \cdot x+b \bmod m$				
	楕円曲線の 定数	記号		備考		
		a		xの係数	一次元	
		b		定数項	一次元	
		m		法	一次元	
マスター 公開鍵	G	Gx	Gのx座標	二次元		
		Gy	Gのy座標			
受信者	受信者 秘密鍵	s		スカラー	一次元	非公開
	受信者 公開鍵	s・G	s・Gx	s・Gのx座標	二次元	公開
			s・Gy	s・Gのy座標		
送信者	暗号化対象 情報	p		任意	一次元	非公開
	中間鍵	P (p・G)	Px=(p・G)x	p・Gのx座標	二次元	
			Py=(p・G)y	p・Gのy座標		
	乱数	r		スカラー	一次元	
	第1送信情報	C1 (r・G)	C1x=(r・G)x	r・Gのx座標	二次元	公開
			C1y=(r・G)y	r・Gのy座標		
	第2送信情報	C2 (P+r・(s・G))	C2x=(P+r・(s・G))x	P+r・(s・G)の x座標	二次元	
			C2y=(P+r・(s・G))y	P+r・(s・G)の y座標		
	第3送信情報	c3	p+Px		一次元	
受信者	第1復号用 情報	s・C1 (s・(r・G))	s・(r・G)x	s・(r・G)の x座標	二次元	
			s・(r・G)y	s・(r・G)の y座標		
	中間鍵(復号)	P (C2-s・C1)	Px=(p・G)x	p・Gのx座標	二次元	
			Py=(p・G)y	p・Gのy座標		
	暗号化対象 情報(復号)	p (c3-Px)		暗号化前と同一		

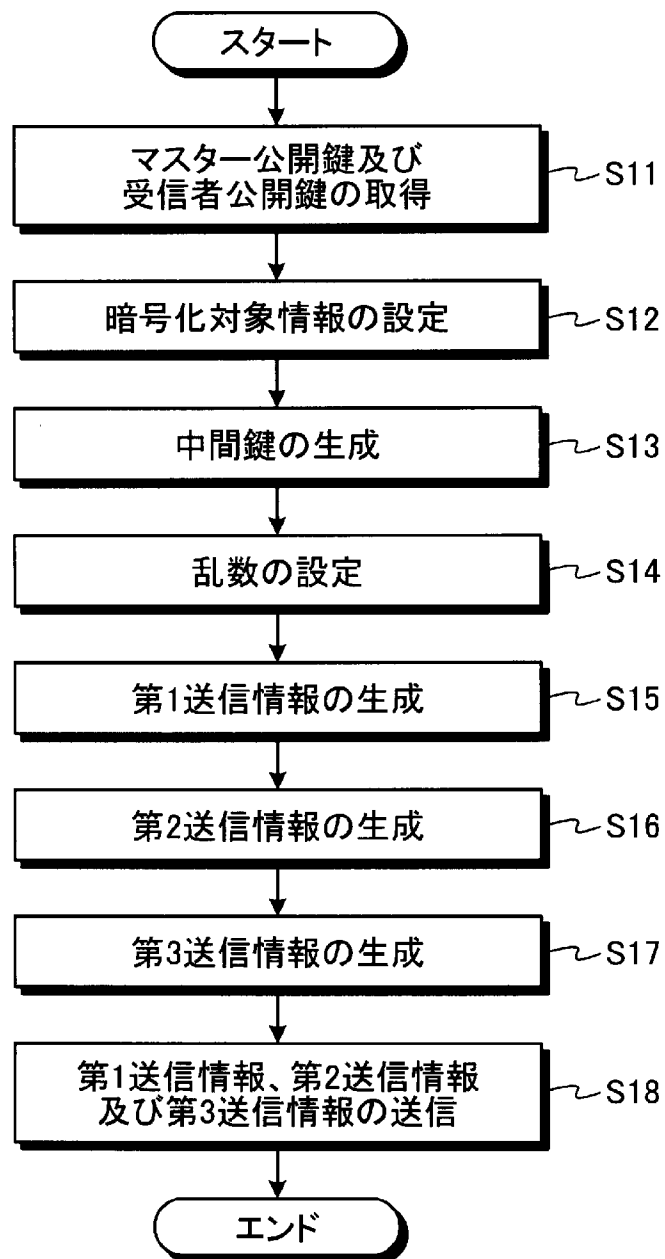
[図5]



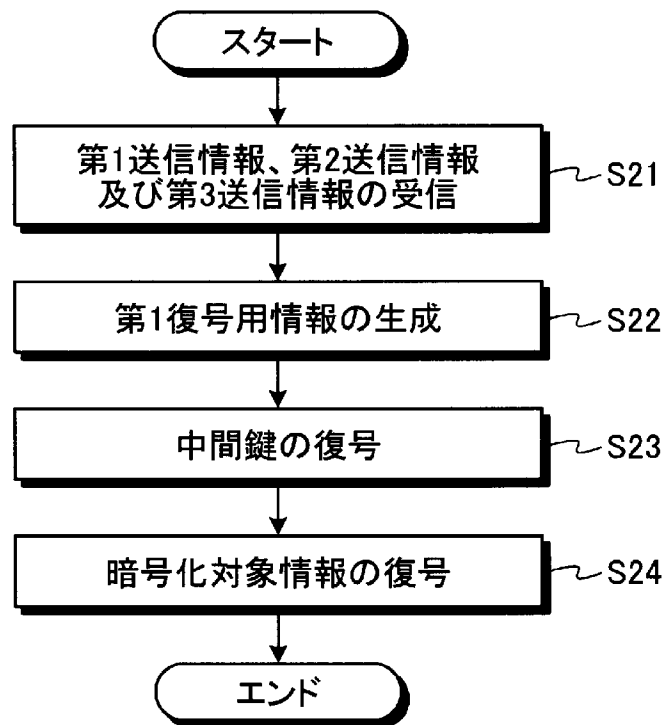
[図6]



[図7]



[図8]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/059771

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i, H04L9/16(2006.01)i, H04L9/30(2006.01)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, H04L9/16, H04L9/30

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	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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	Tatsuaki OKAMOTO et al., Series/Joho Kagaku no Sugaku Gendai Ango, 1st edition, 2nd print, Sangyo Tosho Kabushiki Kaisha, 30 June 1998 (30.06.1998), pages 118 to 122, 202	1-6
Y	JP 11-27256 A (Toyo Communication Equipment Co., Ltd.), 29 January 1999 (29.01.1999), paragraphs [0010], [0012]; fig. 1 (Family: none)	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
01 June 2016 (01.06.16)

Date of mailing of the international search report
14 June 2016 (14.06.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/059771

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-268072 A (Hitachi, Ltd.), 28 September 2001 (28.09.2001), paragraphs [0171] to [0183] & US 6666381 B1 column 24, line 61 to column 26, line 45 & EP 1134653 A2 & DE 60136988 D & AU 2801901 A & TW 569103 B & AU 782868 B & KR 10-2001-0091939 A & AU 2005203004 A	1-6

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L9/08(2006.01)i, H04L9/16(2006.01)i, H04L9/30(2006.01)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（IPC））

Int.Cl. H04L9/08, H04L9/16, H04L9/30

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	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016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	岡本 龍明 他, シリーズ／情報科学の数学 現代暗号, 初版第2刷, 産業図書株式会社, 1998.06.30, p. 118-122、202	1-6
Y	JP 11-27256 A（東洋通信機株式会社）1999.01.29, 段落 [0010]、[0012]、[図1] （ファミリーなし）	1-6

☒ 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

01.06.2016

国際調査報告の発送日

14.06.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

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）

青木 重徳

5 S

4 2 2 9

電話番号 03-3581-1101 内線 3546

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	JP 2001-268072 A (株式会社日立製作所) 2001. 09. 28, 段落 [0 1 7 1] – [0 1 8 3] & US 6666381 B1, 第 2 4 欄第 6 1 行 – 第 2 6 欄第 4 5 行 & EP 1134653 A2 & DE 60136988 D & AU 2801901 A & TW 569103 B & AU 782868 B & KR 10-2001-0091939 A & AU 2005203004 A	1 – 6