(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-141618
(P2010-141618A)
(43)公開日　平成22年6月24日(2010.6.24)

| (51)Int.Cl. | | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| H04L | 9/08 | (2006.01) | H04L | 9/00 | 601B | 5J104 |
| H04L | 9/14 | (2006.01) | H04L | 9/00 | 601F | |
| G09C | 1/00 | (2006.01) | H04L | 9/00 | 641 | |
| | | | G09C | 1/00 | 620B | |
| | | | H04L | 9/00 | 601E | |

審査請求 未請求　請求項の数 16　ＯＬ　（全 78 頁）

(21)出願番号　特願2008-316289 (P2008-316289)
(22)出願日　平成20年12月11日 (2008.12.11)

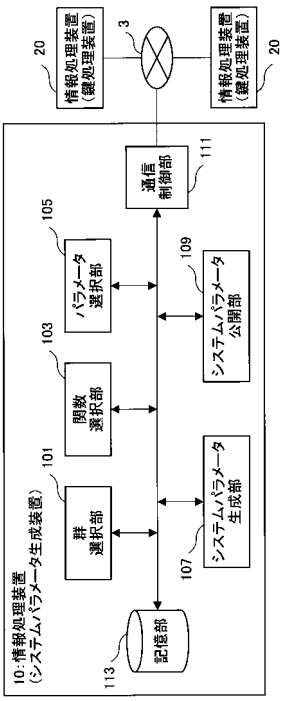
（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(74)代理人　100128587
弁理士　松本　一騎
(72)発明者　樋渡　玄良
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法およびプログラム

(57)【要約】
【課題】暗号化処理量、暗号文サイズを抑制するようにすることが可能な情報処理装置、情報処理方法およびプログラムを提供する。
【解決手段】本発明に係る情報処理装置に、複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成する群選択部と、鍵処理装置で実行される処理に用いられ、複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するパラメータ選択部と、暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択する関数選択部と、を設けた。
【選択図】図１４



【特許請求の範囲】
【請求項１】
複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成する群選択部と、
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するパラメータ選択部と、
前記暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択する関数選択部と、
前記群選択部により選択された巡回群と、前記パラメータ選択部により選択された複数のパラメータと、前記関数選択部により選択された関数と、を用いて、前記複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成するシステムパラメータ生成部と、を備える、情報処理装置。
【請求項２】
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータは、前記鍵処理装置において暗号文の検証処理で用いられる検証用パラメータを生成する際に利用されるパラメータである、請求項１に記載の情報処理装置。
【請求項３】
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータは、前記鍵処理装置において暗号文を生成する際に用いられるセッション鍵を生成する際に利用されるパラメータである、請求項１に記載の情報処理装置。
【請求項４】
前記パラメータ選択部は、
前記群選択部が選択した前記巡回群に属する第１のパラメータを更に選択し、
前記第１のパラメータに対して所定の群演算のみを行なうことにより前記巡回群に属する第２のパラメータを生成する、請求項１に記載の情報処理装置。
【請求項５】
前記パラメータ選択部は、
前記群選択部が選択した前記巡回群に属する第１のパラメータを更に選択し、
前記第１のパラメータを所定の関数に代入することにより得られた値を、前記巡回群に属する第２のパラメータとする、請求項１に記載の情報処理装置。
【請求項６】
前記関数選択部は、所定の群に属する入力値に対して所定の群演算のみを行なっても出力値を生成することが困難である値に前記入力値を変換する変換関数を少なくとも一つ選択し、
前記パラメータ選択部は、前記巡回群から選択された第１のパラメータと、前記変換関数とを用いて、更にパラメータを選択する、請求項５に記載の情報処理装置。
【請求項７】
前記群選択部は、互いに異なる２つの群$G_1$および$G_2$を選択し、
選択された前記群$G_1$および群$G_2$には、群$G_1$から群$G_2$への写像を実現する同型写像が存在する、請求項１に記載の情報処理装置。
【請求項８】
前記関数選択部は、ターゲット衝突困難性を有する関数を選択する、請求項１に記載の情報処理装置。
【請求項９】
前記関数選択部は、定義域から一様分布に入力値を選択すると、出力が値域で一様分布する関数を選択する、請求項８に記載の情報処理装置。
【請求項１０】

他の情報処理装置との間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に用いられるセッション鍵を生成する複数受信者鍵カプセル化メカニズム部と、
前記セッション鍵を用いて前記暗号化通信において送信される暗号文を生成するデータカプセル化メカニズム部と、
を備え、
前記複数受信者鍵カプセル化メカニズム部は、
前記暗号化通信の際に用いられる自装置に固有の公開鍵および秘密鍵を、取得したシステムパラメータに基づいて生成する鍵生成部と、
前記セッション鍵および前記暗号文の検証処理に用いられる検証用パラメータを、前記システムパラメータに基づいて生成する暗号化部と、
前記セッション鍵に関する暗号文を取得して前記システムパラメータに基づいて復号する復号部と、
を有し、
前記システムパラメータは、前記暗号化通信の際に自装置で実行される処理に用いられ、自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータを含み、
前記暗号化部は、前記複数受信者に共通する前記セッション鍵または前記検証用パラメータを生成する、情報処理装置。
【請求項１１】
前記暗号化通信の際に自装置で実行される処理に用いられ、前記自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータは、前記検証用パラメータを生成する際に利用されるパラメータである、請求項１０に記載の情報処理装置。
【請求項１２】
前記暗号化通信の際に自装置で実行される処理に用いられ、前記自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータは、前記セッション鍵を生成する際に利用されるパラメータである、請求項１０に記載の情報処理装置。
【請求項１３】
複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成するステップと、
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するステップと、
前記暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択するステップと、
前記群選択部により選択された巡回群と、前記パラメータ選択部により選択された複数のパラメータと、前記関数選択部により選択された関数と、を用いて、前記複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成するステップと、
を含む、情報処理方法。
【請求項１４】
他の情報処理装置との間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に用いられる自装置に固有の公開鍵および秘密鍵を、取得したシステムパラメータに基づいて生成する鍵生成ステップと、
前記暗号化通信の際に用いられるセッション鍵および暗号文の検証処理に用いられる検証用パラメータを、前記システムパラメータに基づいて生成する暗号化ステップと、
前記セッション鍵に関する暗号文を取得して前記システムパラメータに基づいて復号する復号ステップと、
を含み、
前記システムパラメータは、前記暗号化通信の際に自装置で実行される処理に用いられ

、自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータを含み、
前記暗号化部は、前記複数受信者に共通する前記セッション鍵または前記検証用パラメータを生成する、情報処理方法。
【請求項１５】
コンピュータに、
複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成する群選択機能と、
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するパラメータ選択機能と、
前記暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択する関数選択機能と、
前記群選択部により選択された巡回群と、前記パラメータ選択部により選択された複数のパラメータと、前記関数選択部により選択された関数と、を用いて、前記複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成するシステムパラメータ生成機能と、
を実現させるためのプログラム。
【請求項１６】
他の情報処理装置との間で複数受信者公開鍵暗号技術に基づく暗号化通信を行うことが可能なコンピュータに、
前記暗号化通信の際に自装置で実行される処理に用いられ、自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータを含むシステムパラメータに基づいて、前記暗号化通信の際に用いられる自装置に固有の公開鍵および秘密鍵を生成する機能と、
前記暗号化通信の際に用いられるセッション鍵および暗号文の検証処理に用いられる検証用パラメータを、前記システムパラメータに基づいて生成する機能と、
前記セッション鍵に関する暗号文を取得して前記システムパラメータに基づいて復号する機能と、
を実現させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理方法およびプログラムに関する。
【背景技術】
【０００２】
暗号方式には、共通鍵暗号方式と公開鍵暗号方式の二種類が存在する。共通鍵暗号方式は、通信のために事前の秘密共有が必要となるが、処理が速いという性質がある。他方、公開鍵暗号方式は、通信のための事前の秘密共有は不要であるが、処理が遅いという性質がある。このような性質の違いから、各暗号方式は、それぞれの状況にあった使用が望まれる。
【０００３】
例えば、自社の機器に予め秘密情報を埋め込むことが可能であり、自社の機器同士のみで通信を行う状況では、共通鍵暗号方式の使用が好まれる。また、例えば、インターネット上で赤の他人と秘密情報のやり取りをする場合には、事前の秘密共有ができていない状況も想定されるため、公開鍵暗号方式の使用が好まれる。
【０００４】
近年、インターネットのウェブアプリケーションの発達により、ＳＮＳ、ネットショッピング、ネットオークション等のインターネットを介した個人ユーザ同士のコミュニケー

ションが増加している。上述のようなサービスにおいては、ユーザがプライベートな情報や価値のあるコンテンツを送信する状況も存在しうる。そのような状況では、一対一または一対多での暗号化通信が、ユーザの状況に応じて望まれる状況も考えられる。上述のようなインターネットを介した小規模な市場での一対一、一対多通信の両方に適した暗号方式として、複数受信者公開鍵暗号方式が存在する。この技術は、複数のユーザに暗号文を送信する際、単純にユーザごとの公開鍵暗号処理をするのではなく、共有できる処理をまとめて行なうことで効率化を図る方式である。

【０００５】

ここで、通常、公開鍵暗号方式を用いる暗号方式では、公開鍵暗号方式のみを用いて通信を行なうことは少なく、公開鍵暗号方式を共通鍵暗号方式と組み合わせたハイブリッド暗号方式を用いることが多い。ハイブリッド暗号方式では、処理の速い共通鍵暗号方式で秘密鍵を用いて平文部を暗号化し、暗号化公開鍵暗号方式を用いて共通鍵暗号方式で用いる秘密鍵を暗号化する。このようにすることで、公開鍵暗号方式のみを用いるよりも処理の高速化が見込める。この場合、公開鍵暗号技術を用いて処理する部分を複数受信者鍵カプセル化メカニズム（Ｋｅｙ Ｅｎｃａｐｓｕｌａｔｉｏｎ Ｍｅｃｈａｎｉｓｍ：ＫＥＭ）と呼ぶこととする。また、共通鍵暗号技術を用いて処理する部分を、複数受信者データカプセル化メカニズム（Ｄａｔａ Ｅｎｃａｐｓｕｌａｔｉｏｎ Ｍｅｃｈａｎｉｓｍ：ＤＥＭ）と呼ぶこととする。

【０００６】

複数受信者ＫＥＭでは、安全性はもとより、公開鍵サイズ、秘密鍵サイズ、暗号化処理、復号処理、暗号文サイズ等が重要となってくる。このような観点から複数受信者ＫＥＭとして注目できる方式の一つに、非特許文献１に記載の方式を、既存の手法を用いて複数受信者ＫＥＭにした方式を挙げることができる。この方式は、安全性や効率のバランス面から、優れた方式であるといえる。

【０００７】

【非特許文献１】Ｅ．Ｋｉｌｔｚ，“Ｃｈｏｓｅｎ－ｃｉｐｈｅｒｔｅｘｔ ｓｅｃｕｒｅ ｋｅｙ－ｅｎｃａｐｓｕｌａｔｉｏｎ ｂａｓｅｄ ｏｎ ｇａｐ ｈａｓｈｅｄ ｄｉｆｆｉｅ－ｈｅｌｌｍａｎ” Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｇｒａｐｈｙ，ｖｏｌｕｍｅ ４４５０ ｏｆ Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ，ｐａｇｅｓ ２８２－２９７，Ｓｐｒｉｎｇｅｒ，２００７．

【非特許文献２】Ｇ．Ｈａｎａｏｋａ ａｎｄ Ｋ．Ｋｕｒｏｓａｗａ，“Ｅｆｆｉｃｉｅｎｔ ｃｈｏｓｅｎ ｃｉｐｈｅｒｔｅｘｔ ｓｅｃｕｒｅ ｐｕｂｉｃ ｋｅｙ ｅｎｃｒｙｐｔｉｏｎ ｕｎｄｅｒ ｔｈｅ ｃｏｍｐｕｔａｔｉｏｎａｌ ｄｉｆｆｉｅ－ｈｅｌｌｍａｎ ａｓｓｕｍｐｔｉｏｎ” Ｃｒｙｐｔｏｌｏｇｙ ｅＰｒｉｎｔ Ａｒｃｈｉｖｅ，Ｒｅｐｏｒｔ ２００８／２１１，２００８．ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ／．

【非特許文献３】Ｄ．Ｃａｓｈ，Ｅ．Ｋｉｌｔｚ，Ｖ．Ｓｈｏｕｐ，“Ｔｈｅ Ｔｗｉｎ Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ Ｐｒｏｂｌｅｍ ａｎｄ Ａｐｐｌｉｃａｔｉｏｎｓ” ＥＵＲＯＣＲＹＰＴ，ｖｏｌｕｍｅ ４９６５ ｏｆ Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ，ｐａｇｅｓ １２７－１４５，Ｓｐｒｉｎｇｅｒ，２００８．

【非特許文献４】Ｍ．Ｂａｒｂｏｓａ ａｎｄ Ｐ．Ｆａｒｓｈｉｍ，“Ｒａｎｄｏｍｎｅｓｓ ｒｅｕｓｅ：Ｅｘｔｅｎｓｉｏｎｓ ａｎｄ ｉｍｐｒｏｖｅｍｅｎｔｓ” ＩＭＡ Ｉｎｔ．Ｃｏｎｆ．，ｖｏｌｕｍｅ ４８８７ ｏｆ Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ，ｐａｇｅｓ ２５７－２７６，Ｓｐｒｉｎｇｅｒ，２００７．

【非特許文献５】Ａ．Ｊ．Ｍｅｎｅｚｅｓ，Ｐ．Ｃ．Ｏｏｒｓｃｈｏｔ，Ｓ．Ａ．Ｖａｎｓｔｏｎｅ，“Ｈａｎｄｂｏｏｋ ｏｆ Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ” ＣＲＣ Ｐｒｅｓｓ，２００７．

【発明の開示】

【発明が解決しようとする課題】
【０００８】
しかしながら、上述のような方式において、暗号化処理量および暗号文サイズの効率は、受信者数に比例して大きくなるという問題があった。
【０００９】
そこで、本発明は、このような問題に鑑みてなされたもので、暗号化処理量、暗号文サイズを抑制することが可能な、情報処理装置、情報処理方法およびプログラムを提供することにある。
【課題を解決するための手段】
【００１０】
上記課題を解決するために、本発明のある観点によれば、複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成する群選択部と、前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するパラメータ選択部と、前記暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択する関数選択部と、前記群選択部により選択された巡回群と、前記パラメータ選択部により選択された複数のパラメータと、前記関数選択部により選択された関数と、を用いて、前記複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成するシステムパラメータ生成部と、を備える情報処理装置が提供される。
【００１１】
かかる構成によれば、群選択部は、複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成する。また、パラメータ選択部は、暗号化通信の際に鍵処理装置で実行される処理に用いられ、複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択する。また、関数選択部は、暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択する。また、システムパラメータ生成部は、群選択部により選択された巡回群と、パラメータ選択部により選択された複数のパラメータと、関数選択部により選択された関数と、を用いて、複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成する。
【００１２】
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータは、前記鍵処理装置において暗号文の検証処理で用いられる検証用パラメータを生成する際に利用されるパラメータであってもよい。
【００１３】
前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータは、前記鍵処理装置において暗号文を生成する際に用いられるセッション鍵を生成する際に利用されるパラメータであってもよい。
【００１４】
前記パラメータ選択部は、前記群選択部が選択した前記巡回群に属する第１のパラメータを更に選択し、前記第１のパラメータに対して所定の群演算のみを行なうことにより前記巡回群に属する第２のパラメータを生成してもよい。
【００１５】
前記パラメータ選択部は、前記群選択部が選択した前記巡回群に属する第１のパラメータを更に選択し、前記第１のパラメータを所定の関数に代入することにより得られた値を、前記巡回群に属する第２のパラメータとしてもよい。
【００１６】
前記関数選択部は、所定の群に属する入力値に対して所定の群演算のみを行なっても出

力値を生成することが困難である値に前記入力値を変換する変換関数を少なくとも一つ選択し、前記パラメータ選択部は、前記巡回群から選択された第１のパラメータと、前記変換関数とを用いて、更にパラメータを選択してもよい。

【００１７】

前記群選択部は、互いに異なる２つの群$G_1$および$G_2$を選択し、選択された前記群$G_1$および群$G_2$には、群$G_1$から群$G_2$への写像を実現する同型写像が存在してもよい。

【００１８】

前記関数選択部は、ターゲット衝突困難性を有する関数を選択することが好ましい。

【００１９】

前記関数選択部は、定義域から一様分布に入力値を選択すると、出力が値域で一様分布する関数を選択することが好ましい。

【００２０】

上記課題を解決するために、本発明の別の観点によれば、他の情報処理装置との間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に用いられるセッション鍵を生成する複数受信者鍵カプセル化メカニズム部と、前記セッション鍵を用いて前記暗号化通信において送信される暗号文を生成するデータカプセル化メカニズム部と、を備え、前記複数受信者鍵カプセル化メカニズム部は、前記暗号化通信の際に用いられる自装置に固有の公開鍵および秘密鍵を、取得したシステムパラメータに基づいて生成する鍵生成部と、前記セッション鍵および前記暗号文の検証処理に用いられる検証用パラメータを、前記システムパラメータに基づいて生成する暗号化部と、前記セッション鍵に関する暗号文を取得して前記システムパラメータに基づいて復号する復号部と、を有し、前記システムパラメータは、前記暗号化通信の際に自装置で実行される処理に用いられ、自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータを含み、前記暗号化部は、前記複数受信者に共通する前記セッション鍵または前記検証用パラメータを生成する情報処理装置が提供される。

【００２１】

前記暗号化通信の際に自装置で実行される処理に用いられ、前記自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータは、前記検証用パラメータを生成する際に利用されるパラメータであってもよい。

【００２２】

前記暗号化通信の際に自装置で実行される処理に用いられ、前記自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータは、前記セッション鍵を生成する際に利用されるパラメータであってもよい。

【００２３】

上記課題を解決するために、本発明の更に別の観点によれば、複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成するステップと、前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するステップと、前記暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択するステップと、前記群選択部により選択された巡回群と、前記パラメータ選択部により選択された複数のパラメータと、前記関数選択部により選択された関数と、を用いて、前記複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成するステップと、を含む情報処理方法が提供される。

【００２４】

上記課題を解決するために、本発明の更に別の観点によれば、他の情報処理装置との間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に用いられる自装置に固有の公開鍵および秘密鍵を、取得したシステムパラメータに基づいて生成する鍵生成ステッ

プと、前記暗号化通信の際に用いられるセッション鍵および暗号文の検証処理に用いられる検証用パラメータを、前記システムパラメータに基づいて生成する暗号化ステップと、前記セッション鍵に関する暗号文を取得して前記システムパラメータに基づいて復号する復号ステップと、を含み、前記システムパラメータは、前記暗号化通信の際に自装置で実行される処理に用いられ、自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータを含み、前記暗号化部は、前記複数受信者に共通する前記セッション鍵または前記検証用パラメータを生成する情報処理方法が提供される。

【００２５】

上記課題を解決するために、本発明の更に別の観点によれば、コンピュータに、複数の鍵処理装置間で行われる複数受信者公開鍵暗号技術に基づく暗号化通信の際に利用される巡回群を生成する群選択機能と、前記暗号化通信の際に前記鍵処理装置で実行される処理に用いられ、前記複数の鍵処理装置それぞれに固有の秘密情報を含まず当該複数の鍵処理装置それぞれで共通して用いられるパラメータを含む複数のパラメータを選択するパラメータ選択機能と、前記暗号化通信における暗号文の生成または復号に関する処理に使用され、所定の写像を実現する関数を選択する関数選択機能と、前記群選択部により選択された巡回群と、前記パラメータ選択部により選択された複数のパラメータと、前記関数選択部により選択された関数と、を用いて、前記複数受信者公開鍵暗号技術に利用されるシステムパラメータを生成するシステムパラメータ生成機能と、を実現させるためのプログラムが提供される。

【００２６】

上記課題を解決するために、本発明の更に別の観点によれば、他の情報処理装置との間で複数受信者公開鍵暗号技術に基づく暗号化通信を行うことが可能なコンピュータに、前記暗号化通信の際に自装置で実行される処理に用いられ、自装置および他の情報処理装置それぞれに固有の秘密情報を含まず自装置および他の情報処理装置それぞれで共通して用いられるパラメータを含むシステムパラメータに基づいて、前記暗号化通信の際に用いられる自装置に固有の公開鍵および秘密鍵を生成する機能と、前記暗号化通信の際に用いられるセッション鍵および暗号文の検証処理に用いられる検証用パラメータを、前記システムパラメータに基づいて生成する機能と、前記セッション鍵に関する暗号文を取得して前記システムパラメータに基づいて復号する機能と、を実現させるためのプログラムが提供される。

【発明の効果】

【００２７】

本発明によれば、暗号化処理量、暗号文サイズを抑制することが可能である。

【発明を実施するための最良の形態】

【００２８】

以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【００２９】

なお、説明は、以下の順序で行うものとする。

【００３０】

＜目的＞

以下で説明する本発明の各実施形態に係る情報処理装置および情報処理方法は、上述の複数受信者ＫＥＭに関するものである。本発明の各実施形態に係る情報処理装置および情報処理方法について説明するに先立ち、複数受信者公開鍵暗号方式が置かれている現状について説明しながら、本発明が目的とするところについて、詳細に説明する。

【００３１】

本発明で着目している複数受信者公開鍵暗号方式は、複数のユーザに暗号文を送信する際、単純にユーザごとに公開鍵暗号処理をするのではなく、共有できる処理をまとめて行なうことで効率化を図った方式である。ここで、実行される処理の効率化を図るために、公開鍵暗号技術と共通鍵暗号技術とを組み合わせたハイブリッド型技術が用いられる。

【００３２】

なお、複数受信者公開鍵暗号技術と類似する技術として、ｐｕｂｌｉｃ－ｋｅｙ ｂｒｏａｄｃａｓｔ ｅｎｃｒｙｐｔｉｏｎ ｓｃｈｅｍｅという技術が存在する。これらの技術は、想定している利用状況に違いがある。すなわち、ｐｕｂｌｉｃ－ｋｅｙ ｂｒｏａｄｃａｓｔ ｅｎｃｒｙｐｔｉｏｎ ｓｃｈｅｍｅでは、システムの管理者に大きな負担がかかる大掛かりな大規模システムを想定している。他方、複数受信者公開鍵暗号技術では、システム構成後は管理者が不要となる、手軽な小規模システムを想定している。

【００３３】

ｐｕｂｌｉｃ－ｋｅｙ ｂｒｏａｄｃａｓｔ ｅｎｃｒｙｐｔｉｏｎ ｓｃｈｅｍｅでは、基本的にユーザがシステムに加入するたびに、管理者が鍵生成を行い、生成した鍵をユーザに渡さなければならない。そのため、システムの管理者は、システム構成中はシステムを管理する必要がある。他方、複数受信者公開鍵暗号では、一度システムを構築してしまえば、ユーザは自分一人で鍵生成を行うことが可能であり、自由にシステムに加入できる。このことから、システムの管理者は、初めにシステムを構築してしまえば、管理の必要はない。ただし、複数受信者公開鍵暗号では、受信者が増えれば増える程システムの効率が低下するため、大多数に暗号文を送信するような状況には適さない。

【００３４】

そこで、本発明の各実施形態に係る情報処理装置および情報処理方法では、暗号化処理量を約半分程度に抑制し、暗号文サイズも半分程度に抑制することが可能な、情報処理装置、情報処理方法およびプログラムを提供することを目的とする。

【００３５】

＜本発明の基盤となる技術について＞

まず、本発明に係る各実施形態について詳細なる説明をするに先立ち、図１～図１３を参照しながら、本発明の各実施形態を実現する上で基盤を成す技術的事項について述べる。なお、本発明の各実施形態は、以下に記載する基盤技術の上に改良を加えることにより、より顕著な効果を得ることができるように構成されたものである。従って、その改良に係る技術こそが本発明の各実施形態の特徴を成す部分である。つまり、本発明の各実施形態は、ここで述べる技術的事項の基礎概念を踏襲するが、その本質はむしろ改良部分に集約されており、その構成が明確に相違すると共に、その効果において基盤技術とは一線を画するものであることに注意されたい。

【００３６】

［公開鍵暗号システムについて］

まず、図１～図３を参照しながら、公開鍵暗号システムについて説明する。図１～図３は、公開鍵暗号システムについて説明するための説明図である。

【００３７】

公開鍵暗号システムを用いる各ユーザは、例えば図１に示したように、各自でシステムパラメータと呼ばれる様々なパラメータを設定し、システムパラメータの設定後に各自が使用する秘密鍵および公開鍵を生成する。システムパラメータは、公開鍵暗号システムで用いられるハッシュ（ｈａｓｈ）関数、および、各種の演算に用いられる群や双線形写像などの、ユーザの秘密情報を含まないパラメータである。続いて、公開鍵暗号システムに参加する各ユーザは、各自が決定したシステムパラメータと、公開鍵とを公開する。

【００３８】

例えば、図１に示した例では、ユーザ１は、システムパラメータ$I_1$を設定し、公開鍵$pk_1$と、秘密鍵$sk_1$とを生成する。秘密鍵$sk_1$は、ユーザ１のみが知る鍵としてユーザ１が秘匿し、システムパラメータ$I_1$と、公開鍵$pk_1$とを他のユーザに公開する。

【００３９】

同様に、ユーザ２は、システムパラメータ$I_2$、公開鍵$pk_2$、秘密鍵$sk_2$をそれぞれ設定し、システムパラメータ$I_2$および公開鍵$pk_2$を公開する。また、ユーザ３は、システムパラメータ$I_3$、公開鍵$pk_3$、秘密鍵$sk_3$をそれぞれ設定し、システムパラメータ$I_3$および公開鍵$pk_3$を公開する。

【００４０】

また、公開鍵暗号システムを用いてメッセージを送信する際、メッセージの送信者は、受信者が公開している公開鍵とシステムパラメータとを用いて、送信したいメッセージを暗号化する。例えば、図１に示したように、ユーザ１がユーザ２およびユーザ３にメッセージを送信する場合を考える。ユーザ１は、ユーザ２が公開している公開鍵$pk_2$とシステムパラメータ$I_2$とを用いてメッセージ$m_2$を暗号化し、ユーザ２に送信する。同様に、ユーザ１は、ユーザ３が公開している公開鍵$pk_3$とシステムパラメータ$I_3$とを用いてメッセージ$m_3$を暗号化し、ユーザ３に送信する。なお、図１において、Ｅｎｃ（$pk_2$、$m_2$、$I_2$）という表記は、メッセージ$m_2$を、公開鍵$pk_2$およびシステムパラメータ$I_2$を用いて暗号化したものを表す。

【００４１】

また、ユーザは、各自で公開鍵ｐｋおよび秘密鍵ｓｋを生成できるため、新たにシステムに参加を希望するユーザは、任意のタイミングで公開鍵暗号システムに参加できる。例えば図２に示したように、ユーザ４が公開鍵暗号システムに参加を希望する場合には、ユーザ４自身がシステムパラメータ$I_4$を設定し、公開鍵$pk_4$と秘密鍵$sk_4$とを生成した上で、システムパラメータ$I_4$と公開鍵$pk_4$とを公開する。ユーザ３がユーザ４に対してメッセージ$m_4$を送信する場合には、ユーザ３は、ユーザ４が公開している公開鍵$pk_4$とシステムパラメータ$I_4$とを用いてメッセージ$m_4$を暗号化し、ユーザ４に送信する。

【００４２】

また、公開鍵暗号システムで用いられるシステムパラメータは、ユーザの秘密情報を含

まないパラメータであるため、ユーザ間で共有することが可能である。そのため、図３に示したように、公開鍵暗号システムで共通して用いられるシステムパラメータを生成する第三者をシステムパラメータ生成者として設定することができる。また、システムパラメータ生成者は、ユーザとして公開鍵暗号システムに参加することも可能である。

【００４３】

［複数受信者公開鍵暗号システムについて］

次に、図４～図７を参照しながら、複数受信者公開鍵暗号システムについて説明する。図４～図７は、複数受信者公開鍵暗号システムについて説明するための説明図である。

【００４４】

複数受信者公開鍵暗号システム（ｍｕｌｔｉ－ｒｅｃｉｐｉｅｎｔ　ｐｕｂｌｉｃ－ｋｅｙ　ｅｎｃｒｙｐｔｉｏｎ　ｓｙｓｔｅｍ）は、例えば図４に示したように、システムパラメータ生成者が生成したシステムパラメータＩを共有して用いる暗号システムである。

【００４５】

複数受信者公開鍵暗号システムを用いる各ユーザは、例えば図４に示したように、公開されているシステムパラメータＩを用いて、各自が使用する秘密鍵および公開鍵を生成する。続いて、複数受信者公開鍵暗号システムに参加する各ユーザは、各自が決定した公開鍵を公開する。

【００４６】

複数受信者公開鍵暗号システムでは、複数の受信者の公開鍵と共通のシステムパラメータとを用いて、送信したいメッセージを暗号化する。共通のシステムパラメータを利用することで、数人分の暗号化処理を、いっぺんに効率的に行うことが可能である。

【００４７】

例えば図５に示したように、ユーザ１がユーザ２およびユーザ３のそれぞれにメッセージを送信する場合を考える。この場合、ユーザ１は、ユーザ２およびユーザ３の公開鍵$pk_2$、$pk_3$と、共通のシステムパラメータＩと、を用いて、ユーザ２およびユーザ３に送信するメッセージをいっぺんに暗号化する。なお、図５において、ＭＥｎｃ（（$pk_2$、$pk_3$）、（$m_2$、$m_3$）、Ｉ）という表記は、メッセージ$m_2$およびメッセージ$m_3$を、公開鍵$pk_2$、$pk_3$およびシステムパラメータＩを用いて暗号化し、複数受信者に一度に送信したものを表す。

【００４８】

また、複数受信者公開鍵暗号システムでは、$m_2=m_3$のように、複数の受信者に同じメッセージを送信する場合には、このような利用法に特化した、より効率的な暗号化方法を用いることが可能である。

【００４９】

また、ユーザは、共通のシステムパラメータＩを用いて各自で公開鍵ｐｋおよび秘密鍵ｓｋを生成できるため、新たにシステムに参加を希望するユーザは、任意のタイミングで複数受信者公開鍵暗号システムに参加できる。例えば図６に示したように、ユーザ４が複数受信者公開鍵暗号システムに参加を希望する場合には、ユーザ４自身が公開鍵$pk_4$と秘密鍵$sk_4$とを生成した上で、公開鍵$pk_4$とを公開する。ユーザ３がユーザ４に対してメッセージ$m_4$を送信する場合には、ユーザ３は、ユーザ４が公開している公開鍵$pk_4$と共通のシステムパラメータＩとを用いてメッセージ$m_4$を暗号化し、ユーザ４に送信する。

【００５０】

複数受信者公開鍵暗号システムの一例として、一対多通信を行う方式がある。この一対多通信方式の例として、複数の受信者にそれぞれ異なるメッセージを暗号化する方式と、複数の受信者に同一のメッセージを暗号化する方式とがある。

【００５１】

図７に示した例は、ＥｌＧａｍａｌ暗号を基にした複数受信者公開鍵暗号システムである。この方式は、各ユーザが設定した公開鍵$pk_i=(g_i、y_i)$を用いて、メッセー

ジｍを暗号化する。しかしながら、この暗号化されたメッセージは、各受信者に宛てたメッセージ全てを含むものであるため、ｎ人にメッセージを送信すると、１人にメッセージを送信した場合に比べてｎ倍の処理が必要となるという問題がある。

【００５２】

［ハイブリッド暗号について］

続いて、図８～図１３を参照しながら、ハイブリッド暗号について、詳細に説明する。図８～図１３は、ハイブリッド暗号について説明するための説明図である。

【００５３】

まず、図８を参照しながら、公開鍵暗号システムの長所と短所について説明する。公開鍵暗号システムは、通信を行うユーザ間で事前の秘密共有が不要であるという長所がある。公開鍵暗号システムでは、図８に示したように、公開鍵ｐｋを用いて送信したい平文を暗号文にし、受信者へと送信する。暗号文を受信した受信者は、自身の秘密鍵ｓｋを用いて、暗号文を復号する。

【００５４】

しかしながら、大容量のデータを送信する場合には、処理すべきデータが大きいために、一層の処理時間が必要になるという短所がある。

【００５５】

他方、共通鍵暗号システムは、通信を行うユーザ間で事前の秘密共有が必要であるという短所はあるものの、暗号化処理が早いという長所が存在する。

【００５６】

そこで、公開鍵暗号システムによる処理の内部で共通鍵暗号システムによる処理を行うハイブリッド暗号とすることで、処理の効率化を図ることが可能である。すなわち、共通鍵暗号処理を用いて大容量データを暗号文とするとともに、共通鍵暗号処理に用いる鍵を、公開鍵暗号処理を用いて暗号化する。ここで、公開鍵暗号処理を用いて暗号処理を行う処理部を、鍵カプセル化メカニズム部（以下、ＫＥＭとも称する。）と呼び、共通鍵暗号処理を用いて暗号処理を行う処理部を、データカプセル化メカニズム部（以下、ＤＥＭとも称する。）と呼ぶこととする。

【００５７】

ハイブリッド暗号システムを図解すると、図９のようになる。

送信者は、セッション鍵ｄｋを用いて、送信すべき大容量データをＤＥＭの暗号化処理部（ＤＥＭ．ｅｎｃ）により暗号化する。また、送信者は、セッション鍵ｄｋを、公開鍵ｐｋを用いてＫＥＭの暗号化処理部（ＫＥＭ．ｅｎｃ）により暗号化する。送信者は、セッション鍵ｄｋを暗号化したφと、データを暗号化したχとを、暗号文として送信する。

【００５８】

暗号文の受信者は、暗号文に含まれるφを、秘密鍵ｓｋを用いてＫＥＭの復号処理部（ＫＥＭ．ｄｅｃ）により処理し、セッション鍵ｄｋを生成する。また、暗号文に含まれるχを、生成したセッション鍵ｄｋを用いてＤＥＭの復号処理部（ＤＥＭ．ｄｅｃ）により処理し、データを復号する。

【００５９】

このように、公開鍵暗号システムをハイブリッド化するには、図１０に示したように、装置内に、ＫＥＭとＤＥＭとを設ける。ＫＥＭには、公開鍵ｐｋが入力され、セッション鍵ｄｋは、ＫＥＭのアルゴリズムの内部で生成される乱数を利用して、暗号文と一緒に生成される。また、ＤＥＭには、平文ｍが入力され、ＫＥＭにより生成されたセッション鍵ｄｋを用いて暗号化される。

【００６０】

なお、ＫＥＭは、ハイブリッド暗号を構成する際に、乱数であるセッション鍵を公開鍵暗号技術で暗号化する用途に特化した技術である。また、全ての公開鍵暗号はＫＥＭとして利用可能であるが、全ての公開鍵暗号がＫＥＭとして利用できるとは言えない。

【００６１】

上述のようなハイブリッド方式を、複数受信者公開鍵暗号システムに適用することが可

能である。複数受信者公開鍵システムをハイブリッド化する場合には、図１１～図１３に示したように、主に三種類の方法がある。

【００６２】

第１の方法は、例えば図１１に示したように、複数の受信者に対してそれぞれ異なるメッセージを暗号化して送信する複数受信者公開鍵暗号を、ハイブリッド化するものである。

【００６３】

この第１の方法は、通常の公開鍵暗号方式をハイブリッド化する場合に導入したＫＥＭの換わりに、以下で説明するｍｍＫＥＭ（ｍｕｌｔｉ－ｒｅｃｉｐｉｅｎｔ　ｍｕｌｔｉ－ＫＥＭ）を設ける方法である。

【００６４】

図１１に示したように、ｍｍＫＥＭには、それぞれの受信者の公開鍵$pk_1$～$pk_n$が入力され、それぞれの受信者用のセッション鍵$dk_1$～$dk_n$と、セッション鍵$dk_1$～$dk_n$を暗号化した$\phi_1$～$\phi_n$が出力される。また、ＤＥＭは、それぞれの受信者に向けて送信されるメッセージ$m_1$～$m_n$を、対応するセッション鍵$dk_1$～$dk_n$を用いて暗号化し、$\chi_1$～$\chi_n$を出力する。送信者は、暗号文として、$\phi_1$～$\phi_n$と、$\chi_1$～$\chi_n$とを、一度に複数の受信者に向けて送信する。

【００６５】

第２および第３の方法は、例えば図１２および図１３に示したように、複数の受信者に対して共通のメッセージを暗号化して送信する複数受信者公開鍵暗号を、ハイブリッド化するものである。

【００６６】

第２の方法は、例えば図１２に示したように、疑似乱数生成器（Ｐｓｅｕｄｏ　Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ：ＰＲＮＧ）と、ｍｍＫＥＭと、ＤＥＭと、を用いて、それぞれの受信者用のセッション鍵$dk_1$～$dk_n$を暗号化する。

【００６７】

より詳細には、ＰＲＮＧから出力された一つのセッション鍵ｄｋを、ｍｍＫＥＭから出力されたそれぞれの受信者用のセッション鍵$dk_1$～$dk_n$を利用してＤＥＭにより共通鍵暗号化して、$\chi_1$～$\chi_n$を生成する。また、それぞれの受信者に共通して送信されるメッセージｍを、ＰＲＮＧから出力された一つのセッション鍵ｄｋを用いて共通鍵暗号化し、暗号化されたメッセージ$\chi$を生成する。送信者は、それぞれのセッション鍵$dk_1$～$dk_n$を暗号化した$\phi_1$～$\phi_n$と、共通鍵暗号化処理に用いたセッション鍵ｄｋを暗号化した$\chi_1$～$\chi_n$と、暗号化されたメッセージ$\chi$とを、一度に複数の受信者に向けて暗号文として送信する。

【００６８】

第３の方法は、通常の公開鍵暗号方式をハイブリッド化する場合に導入したＫＥＭの換わりに、以下で説明するｍｓＫＥＭ（ｍｕｌｔｉ－ｒｅｃｉｐｉｅｎｔ　ｓｉｎｇｌｅ－ＫＥＭ）を設ける方法である。

【００６９】

図１３に示したように、ｍｓＫＥＭには、それぞれの受信者の公開鍵$pk_1$～$pk_n$が入力され、それぞれの受信者に共通のセッション鍵ｄｋと、セッション鍵ｄｋをそれぞれの受信者用に暗号化した$\phi_1$～$\phi_n$とが出力される。また、ＤＥＭは、それぞれの受信者に向けて送信される共通のメッセージｍを、セッション鍵ｄｋを用いて暗号化し、暗号化されたメッセージ$\chi$を出力する。送信者は、暗号文として、$\phi_1$～$\phi_n$と、$\chi$とを、一度に複数の受信者に向けて送信する。

【００７０】

このように、それぞれの受信者に対して異なるメッセージを送信するか、共通のメッセージを送信するかに応じて、上述の第１～第３の方法を適宜選択することで、複数受信者公開鍵暗号システムをハイブリッド化することが可能である。

【００７１】

［ラグランジュの補間公式について］

次に、ラグランジュの補間公式について、簡単に説明する。以下で説明する本発明の各実施形態では、二次関数に関するラグランジュの補間公式が用いられる。

【００７２】

一般に、任意の三点が与えられた場合に、これら三点を通る二次関数は、一意に定まる。より詳細には、（$x_1$，f（$x_1$））、（$x_2$，f（$x_2$））、（$x_3$，f（$x_3$））の三点が与えられたとき、二次関数f（x）は、以下の式１のように表せる。ここで、以下の式１で用いられるλは、以下の式２～式４の通りである。

【００７３】

【数１】

$$f(x)=f(x_1)\,\lambda(x_1,x)+f(x_2)\,\lambda(x_2,x)+f(x_3)\,\lambda(x_3,x) \quad \cdots(式１)$$

$$\lambda(x_1,x)=\frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} \quad \cdots(式２)$$

$$\lambda(x_2,x)=\frac{(x-x_1)(x-x_3)}{(x_2-x_1)(x_2-x_3)} \quad \cdots(式３)$$

$$\lambda(x_3,x)=\frac{(x-x_1)(x-x_2)}{(x_3-x_1)(x_3-x_2)} \quad \cdots(式４)$$

【００７４】

すなわち、任意の三点が与えられることで、任意のxに対してf（x）を算出することが可能である。

【００７５】

このラグランジュの補間公式を、本発明の各実施形態では、以下のように適用する。すなわち、素数pを位数に持つ群の生成元をgとし、二次関数f（x）＝$a_0$＋$a_1$x＋$a_2$$x^2$に対して、以下に示す内容が成立する。

【００７６】

生成元gと、任意の三点（$x_1$，$g^{f(x_1)}$）、（$x_2$，$g^{f(x_2)}$）、（$x_3$，$g^{f(x_3)}$）とが与えられた場合に、生成元gの冪に二次関数の係数$a_0$、$a_1$、$a_2$がそれぞれ乗った、以下の式５に示した値を算出することが可能である。

【００７７】

【数２】

$$\left(g^{a_0},g^{a_1},g^{a_2}\right) \quad \cdots(式５)$$

【００７８】

［双線形群における双線形写像について］

続いて、双線形群上の双線形写像に関して説明する。$G_1$、$G_2$、$G_e$を、それぞれ素数pを位数とする巡回群とする。双線形写像eとは、任意の生成元$g_1 \in G_1$、$g_2 \in G_2$およびa，b∈Zpに対して、以下の式６に示す双線形性と、以下の式７に示す非退化性の二つの性質を満たす写像のことをいう。なお、下記式７において、$1_e$は、$G_e$の単位元である。

【００７９】

【数３】

$$e:\mathbf{G}_1\times\mathbf{G}_2\rightarrow\mathbf{G}_e$$

$$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab} \quad \cdots(式６)$$

$$e(g_1,g_2)\neq 1_e \quad \cdots(式７)$$

【００８０】

なお、双線形写像は、Ｇ$_1$とＧ$_2$との関係性から、大きく分けて以下の三種類に分類できる。

【００８１】

・Ｇ$_1$，Ｇ$_2$が同一の群である場合の双線形写像

・Ｇ$_1$，Ｇ$_2$は異なる群であるが、ψ：Ｇ$_1$→Ｇ$_2$という効率的な同型写像が存在する場合の双線形写像

・Ｇ$_1$，Ｇ$_2$は異なる群であり、ψ：Ｇ$_1$→Ｇ$_2$という効率的な同型写像が存在しない場合の双線形写像

【００８２】

以上説明したような基盤技術を踏まえながら、以下では、本発明の各実施形態に係る情報処理装置および情報処理方法について、詳細に説明する。

【００８３】

（第１の実施形態）

＜情報処理装置の構成について＞

以下に、図１４～図１６を参照しながら、本発明の第１の実施形態に係る情報処理装置の構成について詳細に説明する。図１４は、システムパラメータ生成装置として機能する本実施形態に係る情報処理装置の構成を説明するためのブロック図である。図１５および図１６は、鍵処理装置として機能する本実施形態に係る情報処理装置の構成を説明するためのブロック図である。

【００８４】

［システムパラメータ生成装置の構成について］

まず、図１４を参照しながら、システムパラメータ生成者が使用するシステムパラメータ生成装置として機能する本実施形態に係る情報処理装置１０の構成について、詳細に説明する。

【００８５】

本実施形態に係る情報処理装置１０は、例えば、群選択部１０１と、関数選択部１０３と、パラメータ選択部１０５と、システムパラメータ生成部１０７と、システムパラメータ公開部１０９と、通信制御部１１１と、記憶部１１４と、を主に備える。

【００８６】

群選択部１０１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等から構成されている。群選択部１０１は、入力されたセキュリティパラメータ$1^k$に基づいて、ｋビットの素数ｐを、乱数等を用いて無作為に選択する。次に、群選択部１０１は、選択した素数ｐを位数とする群Ｇ$_1$、Ｇ$_2$、Ｇ$_e$を選択する。また、群選択部１０１は、Ｇ$_1$×Ｇ$_2$→Ｇ$_e$となる双線形写像ｅをあわせて選択する。ここで、素数ｐのビット数は、必要とするセキュリティレベルに応じて任意の値を設定することが可能であるが、例えば、ｋ＝１６０と設定することができる。

【００８７】

ここで、群選択部１０１が選択する群は、双線形写像が実現できる群であれば、任意の群であってもよい。

【００８８】

群選択部１０１は、選択した素数ｐ、群Ｇ$_1$、Ｇ$_2$、Ｇ$_e$、双線形写像ｅを、後述する

システムパラメータ生成部１０７に伝送する。また、群選択部１０１は、選択した双線形群$G_1$、$G_2$、$G_e$と、決定した双線形写像ｅとを、後述する記憶部１１３に記録してもよい。

【００８９】

関数選択部１０３は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。関数選択部１０３は、群選択部１０１が選択した群を用いて、後述する鍵処理装置が処理を実行する際に使用する各種の関数を選択する。より詳細には、関数選択部１０３は、関数選択部１０３は、例えば、$G_1 \rightarrow Z_p$という写像を実現する関数$H_1$と、$G_1 \rightarrow \{0,1\}^l$という写像を実現する関数$H_2$と、を選択する。ここで、ｌは、関数$H_2$を用いた結果生成される値のビット長であり、必要とするセキュリティレベルに応じて任意の値を設定可能であるが、例えば、ｌ＝１２８（すなわち、１２８ビット）と設定することができる。

【００９０】

関数選択部１０３が選択する二種類の関数は、上述の写像を実現するものであれば、任意の関数を選択することが可能である。また、関数$H_1$および関数$H_2$が以下の性質を満たすものであれば、安全性を証明することが可能となる。

【００９１】

・関数$H_1$が、ターゲット衝突困難性（ｔａｒｇｅｔ　ｃｏｌｌｉｓｉｏｎ　ｒｅｓｉｓｔａｎｔ）という性質を満たす関数ＴＣＲである。

・関数$H_2$が、定義域から一様分布に入力値を選択すると、出力が値域で一様分布する関数Ｈである。

【００９２】

関数選択部１０３は、選択した各種の関数を、後述するシステムパラメータ生成部１０７に伝送する。また、関数選択部１０３は、選択した各種の関数を、後述する記憶部１１３に記録してもよい。

【００９３】

パラメータ選択部１０５は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。パラメータ選択部１０５は、本実施形態に係る情報処理装置１０がシステムパラメータを生成するために用いる様々なパラメータを、所定の方法に基づいて選択する。パラメータ選択部１０５は、各種パラメータを選択する際に、例えば乱数等を利用して無作為に値を決定する。パラメータ選択部１０５は、選択した各種パラメータを、後述するシステムパラメータ生成部１０７に伝送する。また、パラメータ選択部１０５は、選択した各種パラメータを、後述する記憶部１１３に記録してもよい。

【００９４】

システムパラメータ生成部１０７は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。システムパラメータ生成部１０７は、群選択部１０１、パラメータ選択部１０３および関数選択部１０５から伝送された各種データを利用して、複数受信者公開鍵暗号システムにおけるシステムパラメータを生成する。生成されたシステムパラメータは、ＨＤＤやセキュアモジュールを備えたメモリ等から構成される記憶部１１３に記録される。また、システムパラメータ生成部１０７は、生成したシステムパラメータを、後述するシステムパラメータ公開部１０９に伝送する。

【００９５】

システムパラメータ公開部１０９は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。システムパラメータ公開部１０９は、システムパラメータ生成部１０７が生成したシステムパラメータを、通信網３を介して鍵処理装置として機能する情報処理装置２０に配布する。

【００９６】

通信制御部１１１は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ、通信装置等から構成されている。通信制御部１１１は、システムパラメータ生成装置として機能する情報処理装置１０と、鍵処理装置として機能する情報処理装置２０との間で行われる通信を制御する。

【００９７】

記憶部１１３には、群選択部１０１が選択した素数ｐ、群および双線形写像と、関数選択部１０３が選択した各種関数と、パラメータ選択部１０５が選択した各種パラメータと、が記録される。また、記憶部１１３は、これらの各種データ以外にも、情報処理装置１０が、何らかの処理を行う際に保存する必要が生じた様々なパラメータや処理の途中経過等、または、各種のデータベース等を、適宜記憶することが可能である。この記憶部１１３は、群選択部１０１、関数選択部１０３、パラメータ選択部１０５、システムパラメータ生成部１０７、システムパラメータ公開部１０９、通信制御部１１１等が、自由に読み書きを行うことが可能である。

【００９８】

なお、情報処理装置１０が接続可能な通信網３は、システムパラメータ生成装置として機能する情報処理装置１０と、鍵処理装置として機能する情報処理装置２０とを、双方向通信又は一方向通信可能に接続する通信回線網である。この通信網は、例えば、インターネット、電話回線網、衛星通信網、同報通信路等の公衆回線網や、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＩＰ－ＶＰＮ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ－Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）、ワイヤレスＬＡＮ等の専用回線網などで構成されており、有線／無線を問わない。

【００９９】

以上、本実施形態に係る情報処理装置１０の機能の一例を示した。上記の各構成要素は、汎用的な部材や回路を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。また、各構成要素の機能を、ＣＰＵ等が全て行ってもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用する構成を変更することが可能である。

【０１００】

なお、上述のような本実施形態に係る情報処理装置の各機能を実現するためのコンピュータプログラムを作製し、パーソナルコンピュータ等に実装することが可能である。また、このようなコンピュータプログラムが格納された、コンピュータで読み取り可能な記録媒体も提供することができる。記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリなどである。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信してもよい。

【０１０１】

［鍵処理装置の構成について］

次に、図１５および図１６を参照しながら、複数受信者公開鍵暗号システムを利用する各ユーザが使用する鍵処理装置として機能する本実施形態に係る情報処理装置２０の構成について、詳細に説明する。

【０１０２】

本実施形態に係る情報処理装置２０は、例えば、複数受信者鍵カプセル化メカニズム部（ｍＫＥＭ）２０１と、データカプセル化メカニズム部（ＤＥＭ）２０３と、通信制御部２０５と、記憶部２０７と、を主に備える。

【０１０３】

ｍＫＥＭ２０１は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。ｍＫＥＭ２０１は、メッセージの送信対象である受信者の公開鍵を用いて、公開鍵暗号処理に基づく演算を行い、送信するメッセージを暗号化するためのセッション鍵を生成する。また、ｍＫＥＭ２０１は、生成したセッション鍵を暗号化して、後述する通信制御部２０５を介して、送信者が使用している情報処理装置２０に暗号化したセッション鍵を伝送する。また、ｍＫＥＭ２０１は、生成したセッション鍵を、後述するＤＥＭ２０３に伝送する。このｍＫＥＭ２０１については、以下で改めて詳細に説明する。

【０１０４】

ＤＥＭ２０３は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。ＤＥＭ２０３は、ｍＫＥＭ２０１から伝送されたセッション鍵を用いて、受信者に送信するメッセー

ジを、共通鍵暗号処理に基づいて暗号化する。また、ＤＥＭ２０３は、暗号化されたメッセージを、後述する通信制御部２０５を介して、他の情報処理装置（鍵処理装置）２０に伝送する。なお、ＤＥＭ２０３で行われる共通鍵暗号処理としては、例えば、送信するメッセージ等の特性や各種の条件に応じて、任意の方法を選択することが可能である。

【０１０５】

通信制御部２０５は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ、通信装置等から構成されている。通信制御部２０５は、システムパラメータ生成装置として機能する情報処理装置１０との間で行われる通信を制御する。また、通信制御部２０５は、受信者が使用する他の情報処理装置２０との間で行われる通信を制御する。

【０１０６】

記憶部２０７には、システムパラメータ生成装置として機能する情報処理装置１０が生成したシステムパラメータが、記録される。また、記憶部２０７は、システムパラメータ以外にも、情報処理装置２０が、何らかの処理を行う際に保存する必要が生じた様々なパラメータや処理の途中経過等、または、各種のデータベース等を、適宜記憶することが可能である。この記憶部２０７は、ｍＫＥＭ２０１、ＤＥＭ２０３、通信制御部２０５等が、自由に読み書きを行うことが可能である。

【０１０７】

続いて、図１６を参照しながら、本実施形態に係る情報処理装置２０が備えるｍＫＥＭ２０１について、詳細に説明する。

【０１０８】

本実施形態に係る情報処理装置２０は、例えば図１６に示したように、鍵生成部２１１と、暗号化部２２１と、復号部２３１と、を主に備える。

【０１０９】

鍵生成部２１１は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。鍵生成部２１１は、システムパラメータ生成装置として機能する情報処理装置１０から取得したシステムパラメータを用いて、情報処理装置２０を所持するユーザが使用する公開鍵ｐｋと秘密鍵ｓｋとを生成する。この鍵生成部２１１は、パラメータ生成部２１３と、秘密鍵生成部２１５と、公開鍵生成部２１７と、公開鍵公開部２１９と、を更に備える。

【０１１０】

パラメータ生成部２１３は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。パラメータ生成部２１３は、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている鍵生成方法に則って、鍵生成処理に必要となる各種のパラメータを生成する。各種のパラメータの生成に際して、パラメータ生成部２１３は、記憶部２０７等に格納されているシステムパラメータを参照する。パラメータ生成部２１３は、生成した各種のパラメータを、後述する秘密鍵生成部２１５と、公開鍵生成部２１７とに伝送する。

【０１１１】

秘密鍵生成部２１５は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。秘密鍵生成部２１５は、パラメータ生成部２１３から伝送されたパラメータと、記憶部２０７等に格納されているシステムパラメータとを用い、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている鍵生成方法に則って、秘密鍵ｓｋを生成する。秘密鍵生成部２１５は、生成した秘密鍵ｓｋを、記憶部２０７等に格納して秘匿する。

【０１１２】

公開鍵生成部２１７は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。公開鍵生成部２１７は、パラメータ生成部２１３から伝送されたパラメータと、記憶部２０７等に格納されているシステムパラメータとを用い、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている鍵生成方法に則って、公開鍵ｐｋを生成する。公開鍵生成部２１７は、生成した公開鍵ｐｋを、記憶部２０７等に格納するとともに、後述する公開鍵公開部２１９に伝送する。

【０１１３】

公開鍵公開部２１９は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。公開

鍵公開部２１９は、公開鍵生成部２１７から伝送された公開鍵ｐｋを、通信制御部２０５を介して、他の情報処理装置２０に公開する。

【０１１４】

暗号化部２２１は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。暗号化部２２１は、システムパラメータ生成装置として機能する情報処理装置１０から取得したシステムパラメータと、メッセージの受信者が所持している情報処理装置２０が公開している公開鍵ｐｋとを用いて、セッション鍵の生成および暗号化を行う。この暗号化部２２１は、パラメータ選択部２２３と、検証用パラメータ生成部２２５と、セッション鍵生成部２２７と、を更に備える。

【０１１５】

パラメータ選択部２２３は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。パラメータ選択部２２３は、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている暗号化方法に則って、暗号化処理に必要となる各種のパラメータを選択および生成する。各種のパラメータの選択および生成に際して、パラメータ選択部２２３は、記憶部２０７等に格納されているシステムパラメータを参照する。パラメータ選択部２２３は、生成した各種のパラメータを、後述する検証用パラメータ生成部２２５と、セッション鍵生成部２２７とに伝送する。

【０１１６】

検証用パラメータ生成部２２５は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。検証用パラメータ生成部２２５は、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている暗号化方法に則って、メッセージの受信者が復号処理において実行する検証処理に必要となる検証用パラメータを生成する。検証用パラメータ生成部２２５は、検証用パラメータの生成に際して、システムパラメータと、パラメータ選択部２２３から伝送されたパラメータとを利用し、メッセージの受信者が公開している公開鍵ｐｋは利用しない。

【０１１７】

セッション鍵生成部２２７は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。セッション鍵生成部２２７は、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている暗号化方法に則って、ＤＥＭ２０３が実行する共通鍵暗号処理に用いられるセッション鍵を生成する。また、セッション鍵生成部２２７は、生成したセッション鍵を、ＤＥＭ２０３に伝送する。

【０１１８】

暗号化部２２１は、生成した検証用パラメータと、セッション鍵とを、互いに関連づけて、ＤＥＭ２０３で生成される暗号化されたメッセージとともに、通信制御部２０５を介して他の情報処理装置２０に伝送する。すなわち、暗号化部２２１は、情報処理装置２０の所有者がメッセージの送信者となる場合に利用される処理部である。

【０１１９】

復号部２３１は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。復号部２３１は、システムパラメータ生成装置として機能する情報処理装置１０から取得したシステムパラメータと、メッセージの送信者が所持している情報処理装置２０から伝送された暗号文と、自身の秘密鍵ｓｋとを用いて、セッション鍵の復号を行う。この復号部２３１は、パラメータ算出部２３３と、検証部２３５と、セッション鍵算出部２３７と、を更に備える。

【０１２０】

パラメータ算出部２３３は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。パラメータ算出部２３３は、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている復号方法に則って、復号処理に必要となる各種のパラメータを算出する。各種のパラメータの算出に際して、パラメータ算出部２３３は、記憶部２０７等に格納されているシステムパラメータと、メッセージの送信者から送信された情報とを参照する。また、パラメータ算出部２３３は、パラメータの算出に際して、自身の秘密鍵ｓｋを用いるこ

とも可能である。パラメータ算出部２３３は、算出した各種のパラメータを、後述する検証部２３５と、セッション鍵算出部２３７とに伝送する。

【０１２１】

検証部２３５は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。検証部２３５は、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている復号方法に則って、メッセージの送信者から送信された暗号文の検証処理（いわゆるｖａｌｉｄｉｔｙ　ｃｈｅｃｋ）を行う。検証部２３５は、検証の結果、メッセージの送信者から送信された暗号文が正当なものであると判断した場合には、その旨を後述するセッション鍵算出部２３７に伝送する。また、検証部２３５は、検証の結果、メッセージの送信者から送信された暗号文が正当なものではないと判断した場合には、エラーメッセージを出力し、復号処理を終了する。

【０１２２】

セッション鍵算出部２３７は、例えば、ＣＰＵ、ＲＯＭ、ＲＡＭ等から構成されている。セッション鍵算出部２３７は、検証部２３５から検証に成功した旨を示す情報が伝送されると、ｍＫＥＭ２０１が実行する複数受信者公開鍵暗号処理に規定されている復号方法に則って、ＤＥＭ２０３による復号処理に必要となるセッション鍵を算出する。セッション鍵算出部２３７は、セッション鍵の算出に際して、自身の秘密鍵ｓｋと、記憶部２０７等に格納されているシステムパラメータと、メッセージの送信者から送信された情報とを利用する。セッション鍵算出部２３７は、算出したセッション鍵を、ＤＥＭ２０３に伝送する。

【０１２３】

以上、本実施形態に係る情報処理装置２０の機能の一例を示した。上記の各構成要素は、汎用的な部材や回路を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。また、各構成要素の機能を、ＣＰＵ等が全て行ってもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用する構成を変更することが可能である。

【０１２４】

なお、上述のような本実施形態に係る情報処理装置の各機能を実現するためのコンピュータプログラムを作製し、パーソナルコンピュータ等に実装することが可能である。また、このようなコンピュータプログラムが格納された、コンピュータで読み取り可能な記録媒体も提供することができる。記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリなどである。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信してもよい。

【０１２５】

＜本実施形態に係る情報処理方法の基盤となる暗号処理方法について＞

続いて、本実施形態に係る情報処理方法について説明するに先立ち、本実施形態に係る情報処理方法の基盤となる暗号処理方法について、図１７～２０を参照しながら、詳細に説明する。図１７～図２０は、本実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。本実施形態に係る情報処理方法の基盤となる暗号処理方法は、非特許文献１に記載の暗号処理方法を複数受信者ＫＥＭに適用した方法である。

【０１２６】

［システムパラメータ生成方法について］

まず、図１７を参照しながら、本実施形態に係る情報処理方法の基盤となるシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、システムパラメータ生成者が所持する情報処理装置であるシステムパラメータ生成装置において実行される。

【０１２７】

まず、システムパラメータ生成装置は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇ、$G_e$を選択する。また、Ｇ×Ｇ→Ｇ

$_{e}$を実現する双線形写像ｅを選択する（ステップＳ１００１）。
【０１２８】
次に、システムパラメータ生成装置は、Ｇ→Ｚ$_{p}$という写像を実現する関数ＴＣＲと、Ｇ→｛０，１｝$^{l}$という写像を実現する関数Ｈと、を選択する（ステップＳ１００２）。
【０１２９】
続いて、システムパラメータ生成装置は、パラメータｇ∈$_{R}$Ｇを選択する（ステップＳ１００３）。
【０１３０】
次に、システムパラメータ生成装置は、システムパラメータＩをＩ＝（ｐ，Ｇ，Ｇ$_{e}$，ｇ，ｅ，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ１００４）。
【０１３１】
このような手順を経ることにより、システムパラメータ生成装置は、鍵処理装置の複数受信者ＫＥＭが暗号処理を実行する際に必要となるシステムパラメータを生成することができる。
【０１３２】
［鍵生成方法について］
次に、図１８を参照しながら、本実施形態に係る情報処理方法の基盤となる鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この鍵生成方法は、鍵処理装置を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、鍵処理装置がシステムパラメータ生成装置によって生成されたシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。
【０１３３】
まず、鍵処理装置は、鍵処理装置に固有の秘密情報として、パラメータｘ∈$_{R}$Ｚ$_{p}$を選択する（ステップＳ１０１１）。
【０１３４】
次に、鍵処理装置は、選択したパラメータｘと、システムパラメータとして公開されているｇとを用いて、パラメータｃ＝ｇ$^{x}$を算出する（ステップＳ１０１２）。
【０１３５】
続いて、鍵処理装置は、パラメータｄ∈$_{R}$Ｇを選択する（ステップＳ１０１３）。
【０１３６】
その後、鍵処理装置は、鍵処理装置を所持するユーザに固有の秘密鍵ｓｋ＝（ｘ，ｃ，ｄ）を生成する（ステップＳ１０１４）。また、鍵処理装置は、鍵処理装置を所持するユーザに固有の公開鍵ｐｋ＝（ｃ，ｄ）を生成する（ステップＳ１０１５）。
【０１３７】
その後、鍵処理装置は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ１０１６）。また、生成した公開鍵ｐｋは、他の鍵処理装置に対して公開される。
【０１３８】
このような手順を経ることにより、鍵処理装置は、鍵処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。
【０１３９】
［暗号化方法について］
次に、図１９を参照しながら、本実施形態に係る情報処理方法の基盤となる暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この暗号化方法は、鍵処理装置を所持し、メッセージの送信を行うユーザが、複数受信者ＫＥＭを用いて暗号文を生成する際に実行される。

【０１４０】
まず、鍵処理装置は、パラメータｒ∈$_{R}$Ｚ$_{p}$を無作為に選択する（ステップＳ１０２１）。
【０１４１】
次に、鍵処理装置は、選択したパラメータｒと、システムパラメータとして公開されているパラメータｇとを用いて、パラメータｕ＝ｇ$^{r}$∈Ｇを算出する（ステップＳ１０２２）。
【０１４２】
続いて、鍵処理装置は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈Ｚ$_{p}$を算出する（ステップＳ１０２３）。
【０１４３】
次に、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵ｐｋ$_{i}$（ｉ＝１，・・・ｎ）を用いて、以下の検証用パラメータｖ$_{i}$を算出する（ステップＳ１０２４）。
【０１４４】
【数４】

$$v_i = c_i^{r\alpha} \cdot d_i^{r} \quad \cdots (式１００１)$$

【０１４５】
続いて、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵ｐｋ$_{i}$（ｉ＝１，・・・ｎ）を用いて、以下のセッション鍵ｄｋ$_{i}$を算出する（ステップＳ１０２５）。
【０１４６】
【数５】

$$dk_i = H(c_i^{r}) \in \{0,1\}^{l} \quad \cdots (式１００２)$$

【０１４７】
次に、鍵処理装置は、φ＝（ｕ，ｖ$_{1}$，ｖ$_{2}$，・・・，ｖ$_{n}$）とし、（φ，ｄｋ$_{1}$，ｄｋ$_{2}$，・・・，ｄｋ$_{n}$）を出力する（ステップＳ１０２６）。なお、図１９において、ベクトルｖは、全ての受信者に対するｖ$_{i}$を一括して表記したものを意味する。また、図１９において、ベクトルｄｋは、全ての受信者に対するｄｋ$_{i}$を一括して表記したものを意味する。
【０１４８】
このような手順を経ることにより、鍵処理装置は、鍵処理装置のＤＥＭにおいて実行される共通鍵暗号処理に用いられるセッション鍵ｄｋを生成することができる。
【０１４９】
［復号方法について］
次に、図２０を参照しながら、本実施形態に係る情報処理方法の基盤となる復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置である鍵処理装置において実行される。
【０１５０】
復号処理に先立ち、鍵処理装置は、暗号文の中に含まれるφ＝（ｕ，ｖ$_{1}$，ｖ$_{2}$，・・・，ｖ$_{n}$）の中から、自身に関係する部分（ｕ，ｖ$_{i}$）を抽出する。この抽出処理は、記載されているｖ$_{i}$の順番とユーザとの対応関係とを関連付けるラベルを用いたり、送信者がそれぞれの受信者に必要な情報だけが届くように設定したりすることで実現可能である。
【０１５１】

まず、鍵処理装置は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈$Z_p$を算出する（ステップＳ１０３１）。

【０１５２】

次に、鍵処理装置は、自身の秘密鍵$sk_i$と、システムパラメータと、算出したパラメータαと、暗号文に含まれるｕ，$v_i$とを用いて、暗号文の検証処理を行う。より詳細には、鍵処理装置は、以下の式１００３における等号が成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ１０３２）。

【０１５３】

【数６】

$$e(u, c_i^{\alpha} \cdot d_i) = e(g, v_i) \in G_e \quad \cdots (式１００３)$$

【０１５４】

鍵処理装置は、上記式１００３の等号が成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ１０３３）復号処理を終了する。

【０１５５】

また、上記式１００３の等号が成立した場合には、鍵処理装置は、受信した暗号文が正当なものであると判断し、自身の秘密鍵$sk_i$と、暗号文に含まれるパラメータｕと、システムパラメータとを用いて、自身に対応するセッション鍵$dk_i$＝Ｈ（$u^x$）∈｛０，１｝$^l$を算出する（ステップＳ１０３４）。続いて、鍵処理装置は、算出したセッション鍵$dk_i$を、自装置のＤＥＭへと出力する（ステップＳ１０３５）。

【０１５６】

このような手順を経ることにより、鍵処理装置は、鍵処理装置のＤＥＭにおける復号処理に用いられるセッション鍵ｄｋを算出することができる。

【０１５７】

［基盤技術である暗号処理方法の問題点］

上述のような本実施形態に係る情報処理方法の基盤技術となる暗号処理方法では、以下のような問題点がある。すなわち、基盤技術では、暗号化方法において、それぞれの受信者の公開鍵を用いて検証用パラメータ$v_1$，$v_2$，・・・，$v_n$を計算し、暗号文φに挿入している。暗号文の受信者は、復号方法において、式１００３における等号が成立するか否かを検証することにより、不当な暗号文を排除することが可能となっている。しかしながら、この検証方法を実現するために、受信者数をｎとしたときｎ回のｍｕｌｔｉ－ｓｃａｌａｒ　ｍｕｌｔｉｐｌｉｃａｔｉｏｎの処理が暗号化の際に必要となる。さらに、生成される暗号文においても、ｎ＋１個の要素が必要となる。これらの値が大きいという点が、基盤技術における問題点である。

【０１５８】

＜情報処理方法について＞

本実施形態に係る情報処理方法では、上記問題を解決するために、検証処理を行なうために必要な要素をシステムパラメータに加えることにより、情報処理方法全体における効率化を実現している。これにより、基盤技術の暗号化方法において、受信者ごとに公開鍵を用いたパラメータ生成処理が必要であったものを、全ユーザ共通の要素を用いる処理一回のみで、全ユーザに共通する検証用パラメータを生成することが可能となる。

【０１５９】

以下、本実施形態に係る情報処理方法について、図２１～図２４を参照しながら、詳細に説明する。図２１～図２４は、本実施形態に係る情報処理方法について説明するための流れ図である。

【０１６０】

［システムパラメータ生成方法について］

まず、図２１を参照しながら、本実施形態に係るシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、システムパラメータ生成装置として機能する本実施形態に係る情報処理装置１０において実行される。

【０１６１】

まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群$G_1$、$G_2$、$G_e$を選択する。また、$G_1 \times G_2 \rightarrow G_e$を実現する双線形写像ｅを選択する（ステップＳ１０１）。

【０１６２】

次に、情報処理装置１０の関数選択部１０３は、$G_1 \rightarrow Z_p$という写像を実現する関数ＴＣＲと、$G_1 \rightarrow \{0, 1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ１０２）。

【０１６３】

続いて、情報処理装置１０のパラメータ選択部１０５は、以下の式１０１および式１０２に示すパラメータを選択する（ステップＳ１０３）。

【０１６４】

【数７】

$$g_1 \in_R \mathbf{G}_1 \quad \cdots(\text{式}101)$$

$$g_2, \hat{c}, \hat{d} \in_R \mathbf{G}_2 \quad \cdots(\text{式}102)$$

【０１６５】

次に、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩを以下の式１０３のように構成し、各鍵処理装置に公開する（ステップＳ１０４）。

【０１６６】

【数８】

$$I = \left(p, \mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_e, g_1, g_2, \hat{c}, \hat{d}, e, TCR, H\right) \quad \cdots(\text{式}103)$$

【０１６７】

このような手順を経ることにより、システムパラメータ生成装置として機能する情報処理装置１０は、鍵処理装置として機能する情報処理装置２０のｍＫＥＭ２０１が暗号処理を実行する際に必要となるシステムパラメータを生成することができる。

【０１６８】

なお、上述の群$G_1$および$G_2$について、$G_1$と$G_2$とは同じ群であっても、異なる群であってもよい。$G_1$および$G_2$が同じ群である場合には、$g_1 = g_2$として、以下で説明する処理が実行される。

【０１６９】

［鍵生成方法について］

次に、図２２を参照しながら、本実施形態に係る鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持し、鍵処理装置として機能する情報処理装置２０の鍵生成部２１１において実行される。なお、この鍵生成方法は、情報処理装置２０を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、情報処理装置２０がシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。

【０１７０】

まず、パラメータ生成部２１３は、情報処理装置２０に固有の秘密情報として、パラメータ$x \in_R Z_p$を選択する（ステップＳ１１１）。

【０１７１】

次に、パラメータ生成部２１３は、選択したパラメータｘと、システムパラメータとし

て公開されている$g_1$とを用いて、パラメータ$c = g_1^{x} \in_R G_1$を算出する（ステップＳ１１２）。

【０１７２】

続いて、秘密鍵生成部２１５は、選択したパラメータｘを、情報処理装置２０を所持するユーザに固有の秘密鍵ｓｋとして設定する（ステップＳ１１３）。また、公開鍵生成部２１７は、算出したパラメータｃを、情報処理装置２０を所持するユーザに固有の公開鍵ｐｋとして設定する（ステップＳ１１４）。

【０１７３】

その後、鍵生成部２１１は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ１１５）。また、公開鍵公開部２１９は、生成した公開鍵ｐｋを、他の情報処理装置２０に対して公開する。

【０１７４】

このような手順を経ることにより、情報処理装置２０の鍵生成部２１１は、情報処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。

【０１７５】

［暗号化方法について］

次に、図２３を参照しながら、本実施形態に係る暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持し、鍵処理装置として機能する情報処理装置２０の暗号化部２２１において実行される。なお、この暗号化方法は、情報処理装置２０を所持し、メッセージの送信を行うユーザが、複数受信者ＫＥＭを用いて暗号文を生成する際に実行される。

【０１７６】

まず、パラメータ選択部２２３は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ１２１）。

【０１７７】

次に、パラメータ選択部２２３は、選択したパラメータｒと、システムパラメータとして公開されているパラメータ$g_1$とを用いて、パラメータ$u = g_1^{r} \in G_1$を算出する（ステップＳ１２２）。

【０１７８】

続いて、パラメータ選択部２２３は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ１２３）。

【０１７９】

次に、検証用パラメータ生成部２２５は、メッセージの送信を行う全ての情報処理装置２０に共通する検証用パラメータを、以下の式１１１に基づいて生成する（ステップＳ１２４）。この検証用パラメータは、以下の式１１１から明らかなように、システムパラメータと、パラメータ選択部２２３によって選択されたパラメータとを用いて、生成することが可能である。

【０１８０】

【数９】

$$\hat{v} = \hat{c}^{r\alpha} \cdot \hat{d}^{r} \in \mathbf{G_2} \quad \cdots (式１１１)$$

【０１８１】

続いて、セッション鍵生成部２２７は、メッセージの送信を行う情報処理装置２０全てに対して、送信先の情報処理装置２０の公開鍵$pk_i$（ｉ＝１，・・・ｎ）を用いて、以下のセッション鍵$dk_i$を算出する（ステップＳ１２５）。

【０１８２】

【数１０】

$$dk_i = H(c_i^r) \in \{0,1\}^l \quad \cdots (式１１２)$$

【０１８３】

次に、暗号化部２２１は、以下の式１１３に示すセッション鍵を出力する（ステップＳ１２６）。

【０１８４】

【数１１】

$$(\phi, \overrightarrow{dk}) = (u, \hat{v}, dk_1, dk_2, \cdots, dk_n) \quad \cdots (式１１３)$$

【０１８５】

このような手順を経ることにより、情報処理装置２０は、ＤＥＭ２０３において実行される共通鍵暗号処理に用いられるセッション鍵ｄｋを生成することができる。

【０１８６】

上述のように、基盤技術における暗号化方法では、受信者の公開鍵$pk_i$を用いて各受信者に対して検証用パラメータ$v_i$を算出していたが、本実施形態に係る暗号化方法では、システムパラメータとして公開されている値を用いて検証用パラメータを生成する。これにより、本実施形態に係る暗号化方法では、演算回数の削減を図ることが可能となる。

【０１８７】

［復号方法について］

次に、図２４を参照しながら、本実施形態に係る復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置２０の復号部２３１において実行される。

【０１８８】

まず、パラメータ算出部２３３は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈$Z_p$を算出する（ステップＳ１３１）。

【０１８９】

次に、検証部２３５は、システムパラメータと、算出したパラメータαと、暗号文に含まれるパラメータとを用いて、暗号文の検証処理を行う。より詳細には、検証部２３５は、以下の式１２１における等号が成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ１３２）。

【０１９０】

【数１２】

$$e(u, \hat{c}^{\alpha} \cdot \hat{d}) = e(g_1, \hat{v}) \in G_e \quad \cdots (式１２１)$$

【０１９１】

検証部２３５は、上記式１２１の等号が成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ１３３）復号処理を終了する。

【０１９２】

また、上記式１２１の等号が成立した場合には、検証部２３５は、受信した暗号文が正当なものであると判断し、暗号文が正当なものである旨を示す情報を、セッション鍵算出部２３７に伝送する。セッション鍵算出部２３７は、自身の秘密鍵$sk_i$と、暗号文に含まれるパラメータｕと、システムパラメータとを用いて、自身に対応するセッション鍵$dk_i = H(u^x) \in \{0,1\}^l$を算出する（ステップＳ１３４）。続いて、セッション鍵算出部２３７は、算出したセッション鍵$dk_i$を、自装置のＤＥＭ２０３へと出力する（ステップＳ１３５）。

【０１９３】

このような手順を経ることにより、情報処理装置２０の復号部２３１は、ＤＥＭ２０３における復号処理に用いられるセッション鍵ｄｋを算出することができる。

【０１９４】

上述のように、基盤技術における復号方法では、受信者の公開鍵$pk_i$を用いて検証用パラメータを用いた検証処理を行っていたが、本実施形態に係る復号方法では、システムパラメータとして公開されている値を用いて検証処理を実施する。

【０１９５】

＜暗号化時の計算量と暗号文のサイズについて＞

以下では、本実施形態に係る情報処理方法の暗号化時における計算量と暗号文のサイズについて、基盤技術における暗号処理方法と比較しながら説明する。

【０１９６】

［暗号化時の計算量について］

まず、受信者数をｎとしたときの、基盤技術における暗号化方法での計算量と、本実施形態に係る暗号化方法での計算量を比較する。両方法ともに、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ、および、ｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が支配的となるため、それぞれの演算数の比較を行った。暗号化時の計算量を比較した結果を、以下の表１に示す。

【０１９７】

なお、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎとは、$g^r$のように、一つの群要素に対してｓｃａｌａｒ倍算をすることを意味する。また、ｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎとは、$g_1^{r_1} \cdot g_2^{r_2}$のように、二つの群要素に対して異なる値のｓｃａｌａｒ倍算をすることを意味する。

【０１９８】

【表１】

表１　暗号化時における計算量

| | single-scalar multiplication | multi-scalar multiplication |
|---|---|---|
| 基盤技術 | ｎ＋１ | ｎ |
| 本実施形態 | ｎ＋１ | １ |

【０１９９】

表１より、基盤技術における暗号化方法では、（ｎ＋１）回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。また、本実施形態に係る暗号化方法では、（ｎ＋１）回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、１回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。すなわち、本実施形態に係る暗号化方法では、（ｎ－１）回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎを削減できたことが分かる。

【０２００】

非特許文献５に記載のように、一般的にｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎは、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの１．５倍の処理が必要であると考えられている。このことを考慮すると、基盤技術における暗号化方法では（２．５ｎ＋１）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が必要である。他方、本実施形態に係る暗号化方式では、（ｎ＋２．５）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量で処理が完了することが分かる。

【０２０１】

［暗号文のサイズについて］

次に、受信者数をｎとしたときの、基盤技術における暗号文サイズと、本実施形態に係る情報処理方法における暗号文サイズとを比較する。両方法とも、同じ群を用いていると考え、暗号文に含まれる要素数で比較を行った。得られた結果を、以下の表２に示す。

【０２０２】
【表２】

表２　暗号文のサイズ

| | $G_1$の要素数 | $G_2$の要素数 |
|---|---|---|
| 基盤技術 | 1 | n |
| 本実施形態 | 1 | 1 |

【０２０３】
表２より、基盤技術では、$G_1$と$G_2$の要素を合わせてｎ＋１個の要素が存在するのに対し、本実施形態では、受信者数に依存せずに、要素数は２個となる。この結果から明らかなように、本実施形態に係る情報処理方法では、暗号文のサイズを、受信者数に依存せずに、一定のサイズにすることができる。
【０２０４】
＜第１変形例について＞
本実施形態に係るシステムパラメータ生成方法において、ψ：$G_1 \rightarrow G_2$となる効率的な同型写像が存在するように、情報処理装置１０の群選択部１０１が群$G_1$，$G_2$を選択する場合を考える。この場合、情報処理装置２０の復号部２３１（より詳細には、検証部２３５）で実行される双線形写像の値を算出する以外の演算を、全て群$G_1$上で行なうことが可能となり、暗号文も、$G_1$上の要素のみで表すことが可能となる。さらに、群$G_1$，$G_2$の選択方法として、$G_2$上の演算よりも$G_1$上での演算の方が軽く、また要素の表現サイズに関しても、$G_2$よりも$G_1$の方が小さく表現可能となる場合も考えられる。
【０２０５】
このような場合、本実施形態にかかる計算量と暗号文サイズの削減が実現可能となる。上述のような変形例を実現するためには、本発明の第１の実施形態に係るシステムパラメータ生成方法、暗号化方法および復号方法を、以下のように変形する。
【０２０６】
［システムパラメータ生成方法について］
まず、図２５を参照しながら、本変形例に係るシステムパラメータ生成方法について、詳細に説明する。図２５は、本変形例に係るシステムパラメータ生成方法を説明するための流れ図である。
【０２０７】
まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ψ：$G_1 \rightarrow G_2$となる効率的な同型写像が存在するように、ｐを位数とする群$G_1$、$G_2$、$G_e$を選択する。また、$G_1 \times G_2 \rightarrow G_e$を実現する双線形写像ｅを選択する（ステップＳ１４１）。
【０２０８】
次に、情報処理装置１０の関数選択部１０３は、$G_1 \rightarrow Z_p$という写像を実現する関数ＴＣＲと、$G_1 \rightarrow \{0, 1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ１０２）。
【０２０９】
続いて、情報処理装置１０のパラメータ選択部１０５は、以下の式１３１に示すパラメータを選択する（ステップＳ１４２）。
【０２１０】
【数１３】

$$g_1, \hat{c}, \hat{d} \in_R G_1 \quad \cdots (式１３１)$$

【０２１１】
次に、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩを以下の式１３２のように構成し、各鍵処理装置に公開する（ステップＳ１４３）。

【０２１２】
【数１４】

$$I=\left(p,\mathbf{G_1},\mathbf{G_2},\mathbf{G_e},g_1,\hat{c},\hat{d},e,TCR,H\right) \quad \cdots(式１３２)$$

【０２１３】
［暗号化方法について］
次に、図２６を参照しながら、本変形例に係る暗号化方法について、詳細に説明する。図２６は、本変形例に係る暗号化方法を説明するための流れ図である。
【０２１４】
まず、パラメータ選択部２２３は、パラメータ$r\in_R Z_p$を無作為に選択する（ステップＳ１２１）。
【０２１５】
次に、パラメータ選択部２２３は、選択したパラメータｒと、システムパラメータとして公開されているパラメータ$g_1$とを用いて、パラメータ$u=g_1{}^r\in G_1$を算出する（ステップＳ１２２）。
【０２１６】
続いて、パラメータ選択部２２３は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha=TCR(u)\in Z_p$を算出する（ステップＳ１２３）。
【０２１７】
次に、検証用パラメータ生成部２２５は、メッセージの送信を行う全ての情報処理装置２０に共通する検証用パラメータを、以下の式１３３に基づいて生成する（ステップＳ１４４）。この検証用パラメータは、以下の式１３３から明らかなように、システムパラメータと、パラメータ選択部２２３によって選択されたパラメータとを用いて、群$G_1$上での演算を用いて生成することが可能である。
【０２１８】
【数１５】

$$\hat{v}=\hat{c}^{r\alpha}\cdot\hat{d}^{r}\in\mathbf{G_1} \quad \cdots(式１３３)$$

【０２１９】
続いて、セッション鍵生成部２２７は、メッセージの送信を行う情報処理装置２０全てに対して、送信先の情報処理装置２０の公開鍵$pk_i$（ｉ＝１，・・・ｎ）を用いて、以下のセッション鍵$dk_i$を算出する（ステップＳ１２５）。
【０２２０】
【数１６】

$$dk_i=H(c_i^r)\in\{0,1\}^l \quad \cdots(式１１２)$$

【０２２１】
次に、暗号化部２２１は、以下の式１１３に示すセッション鍵を出力する（ステップＳ１２６）。
【０２２２】
【数１７】

$$(\phi,\overrightarrow{dk})=(u,\hat{v},dk_1,dk_2,\cdots,dk_n) \quad \cdots(式１１３)$$

【０２２３】
［復号方法について］
次に、図２７を参照しながら、本変形例に係る復号方法について、詳細に説明する。図

２７は、本変形例に係る復号方法を説明するための流れ図である。

【０２２４】

まず、パラメータ算出部２３３は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈$Z_p$を算出する（ステップＳ１３１）。

【０２２５】

次に、検証部２３５は、システムパラメータと、算出したパラメータαと、暗号文に含まれるパラメータとを用いて、暗号文の検証処理を行う。より詳細には、検証部２３５は、以下の式１３４における等号が成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ１４５）。

【０２２６】

【数１８】

$$e(u,\psi(\hat{c}^{\alpha}\cdot\hat{d}))=e(g_1,\psi(\hat{v}))\in G_e \quad \cdots(式１３４)$$

【０２２７】

上記式１３４から明らかなように、同型写像ψを用いて群$G_1$上の要素を群$G_2$上に写像することで、双線形写像ｅの演算を行なうことができる。

【０２２８】

検証部２３５は、上記式１３４の等号が成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ１３３）復号処理を終了する。

【０２２９】

また、上記式１３４の等号が成立した場合には、検証部２３５は、受信した暗号文が正当なものであると判断し、暗号文が正当なものである旨を示す情報を、セッション鍵算出部２３７に伝送する。セッション鍵算出部２３７は、自身の秘密鍵$sk_i$と、暗号文に含まれるパラメータｕと、システムパラメータとを用いて、自身に対応するセッション鍵$dk_i=H(u^x)\in\{0,1\}^l$を算出する（ステップＳ１３４）。続いて、セッション鍵算出部２３７は、算出したセッション鍵$dk_i$を、自装置のＤＥＭ２０３へと出力する（ステップＳ１３５）。

【０２３０】

以上説明したように、本発明の第１の実施形態に係る情報処理装置および情報処理方法では、鍵処理装置として機能する情報処理装置２０におけるｍＫＥＭ２０１として、図１１に示したｍｍＫＥＭを導入することで、複数受信者公開鍵暗号システムを実現している。

【０２３１】

（第２の実施形態）

続いて、図２８～図３７を参照しながら、本発明の第２の実施形態に係る情報処理装置および情報処理方法について、詳細に説明する。

【０２３２】

＜情報処理装置の構成について＞

まず、本実施形態に係る情報処理装置の構成について、説明する。本実施形態に係る情報処理装置は、システムパラメータ生成装置として機能する情報処理装置１０と、鍵処理装置として機能する情報処理装置２０とが存在する。

【０２３３】

ここで、本実施形態におけるシステムパラメータ生成装置として機能する情報処理装置１０は、図１４に示した本発明の第１の実施形態に係る情報処理装置１０の構成を有し、各処理部で実行される処理内容のみが異なるものである。そのため、本実施形態に係る情報処理装置１０が備える各処理部の機能については、以下で本実施形態に係る情報処理方法を説明しながら説明するものとする。

【０２３４】

同様に、本実施形態における鍵処理装置として機能する情報処理装置２０は、図１５および図１６に示した本発明の第１の実施形態に係る情報処理装置２０の構成を有し、各処理部で実行される処理内容のみが異なるものである。そのため、本実施形態に係る情報処理装置２０が備える各処理部の機能については、以下で本実施形態に係る情報処理方法を説明しながら説明するものとする。

【０２３５】

＜本実施形態に係る情報処理方法の基盤となる暗号処理方法について＞

続いて、本実施形態に係る情報処理方法について説明するに先立ち、本実施形態に係る情報処理方法の基盤となる暗号処理方法について、図２８～３１を参照しながら、詳細に説明する。図２８～図３１は、本実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。本実施形態に係る情報処理方法の基盤となる暗号処理方法は、非特許文献２に記載の暗号処理方法である。

【０２３６】

［システムパラメータ生成方法について］

まず、図２８を参照しながら、本実施形態に係る情報処理方法の基盤となるシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、システムパラメータ生成者が所持する情報処理装置であるシステムパラメータ生成装置において実行される。

【０２３７】

まず、システムパラメータ生成装置は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ２００１）。

【０２３８】

次に、システムパラメータ生成装置は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0, 1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ２００２）。

【０２３９】

続いて、システムパラメータ生成装置は、パラメータ$g \in_R G$を選択する（ステップＳ２００３）。

【０２４０】

次に、システムパラメータ生成装置は、システムパラメータＩをＩ＝（ｐ，Ｇ，ｇ，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ２００４）。

【０２４１】

このような手順を経ることにより、システムパラメータ生成装置は、鍵処理装置の複数受信者ＫＥＭが暗号処理を実行する際に必要となるシステムパラメータを生成することができる。

【０２４２】

［鍵生成方法について］

次に、図２９を参照しながら、本実施形態に係る情報処理方法の基盤となる鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この鍵生成方法は、鍵処理装置を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、鍵処理装置がシステムパラメータ生成装置によって生成されたシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。

【０２４３】

まず、鍵処理装置は、鍵処理装置に固有の秘密情報として、パラメータ$a_0, a_1, a_2 \in_R Z_p$を選択する（ステップＳ２０１１）。本実施形態において、このような３種類のパラメータを選択することは、選択したパラメータを係数に持つ$f(x) = a_0 + a_1 x + a_2 x^2$という二次関数を定義したことと同様の意味を有する。

【０２４４】

次に、鍵処理装置は、選択したパラメータ$a_0, a_1, a_2$と、システムパラメータで

あるｇとを用い、先に説明したラグランジュの補間公式を利用して、以下の式２００１～式２００３に示すパラメータ$y_0$，$y_1$，$y_2$を算出する（ステップＳ２０１２）。

【０２４５】

【数１９】

$$y_0 = g^{a_0} \in G \quad \cdots(式２００１)$$

$$y_1 = g^{a_1} \in G \cdots(式２００２)$$

$$y_2 = g^{a_2} \in G \cdots(式２００３)$$

【０２４６】

その後、鍵処理装置は、鍵処理装置を所持するユーザに固有の秘密鍵ｓｋ＝（$a_0$，$a_1$，$a_2$）を生成する（ステップＳ２０１３）。また、鍵処理装置は、鍵処理装置を所持するユーザに固有の公開鍵ｐｋ＝（$y_0$，$y_1$，$y_2$）を生成する（ステップＳ２０１４）。

【０２４７】

その後、鍵処理装置は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ２０１５）。また、生成した公開鍵ｐｋは、他の鍵処理装置に対して公開される。

【０２４８】

このような手順を経ることにより、鍵処理装置は、鍵処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。

【０２４９】

［暗号化方法について］

次に、図３０を参照しながら、本実施形態に係る情報処理方法の基盤となる暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この暗号化方法は、鍵処理装置を所持し、メッセージの送信を行うユーザが、複数受信者ＫＥＭを用いて暗号文を生成する際に実行される。

【０２５０】

まず、鍵処理装置は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ２０２１）。

【０２５１】

次に、鍵処理装置は、選択したパラメータｒと、システムパラメータとして公開されているパラメータｇとを用いて、パラメータ$u = g^r \in G$を算出する（ステップＳ２０２２）。

【０２５２】

続いて、鍵処理装置は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ２０２３）。

【０２５３】

次に、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵$pk_i$（ｉ＝１，・・・ｎ）を用い、ラグランジュの補間公式を利用して、以下の検証用パラメータ$v_i$を算出する（ステップＳ２０２４）。

【０２５４】

【数２０】

$$v_i = y_{0,i}^{r} \cdot y_{1,i}^{r\alpha} \cdot y_{2,i}^{r\alpha^2} \left(= g^{r \cdot f_i(\alpha)}\right) \quad \cdots(式２００４)$$

【０２５５】

続いて、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵$pk_i$（$i=1,\cdots,n$）を用いて、以下のセッション鍵$dk_i$を算出する（ステップＳ２０２５）。

【０２５６】

【数２１】

$$dk_i = H(y_{0,i}^r) \in \{0,1\}^l \quad \cdots(式２００５)$$

【０２５７】

次に、鍵処理装置は、$\phi=(u, v_1, v_2, \cdots, v_n)$とし、$(\phi, dk_1, dk_2, \cdots, dk_n)$を出力する（ステップＳ２０２６）。

【０２５８】

このような手順を経ることにより、鍵処理装置は、鍵処理装置のＤＥＭにおいて実行される共通鍵暗号処理に用いられるセッション鍵ｄｋを生成することができる。

【０２５９】

［復号方法について］

次に、図３１を参照しながら、本実施形態に係る情報処理方法の基盤となる復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置である鍵処理装置において実行される。

【０２６０】

復号処理に先立ち、鍵処理装置は、暗号文の中に含まれる$\phi=(u, v_1, v_2, \cdots, v_n)$の中から、自身に関係する部分$(u, v_i)$を抽出する。この抽出処理は、記載されている$v_i$の順番とユーザとの対応関係とを関連付けるラベルを用いたり、送信者がそれぞれの受信者に必要な情報だけが届くように設定したりすることで実現可能である。

【０２６１】

まず、鍵処理装置は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha=TCR(u)\in Z_p$を算出する（ステップＳ２０３１）。

【０２６２】

次に、鍵処理装置は、自身の秘密鍵$sk_i$（すなわち、二次関数ｆ（ｘ））と、システムパラメータと、算出したパラメータαと、暗号文に含まれる$u, v_i$とを用いて、暗号文の検証処理を行う。より詳細には、鍵処理装置は、以下の式２００６における等号が成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ２０３２）。

【０２６３】

【数２２】

$$u^{f_i(\alpha)} = v_i \in G \quad \cdots(式２００６)$$

【０２６４】

鍵処理装置は、上記式２００６の等号が成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ２０３３）復号処理を終了する。

【０２６５】

また、上記式２００６の等号が成立した場合には、鍵処理装置は、受信した暗号文が正当なものであると判断し、自身の秘密鍵$sk_i$と、暗号文に含まれるパラメータｕと、システムパラメータとを用いて、自身に対応するセッション鍵$dk_i$を、以下の式２００７を用いて算出する（ステップＳ２０３４）。続いて、鍵処理装置は、算出したセッション鍵$dk_i$を、自装置のＤＥＭへと出力する（ステップＳ２０３５）。

【０２６６】

【数２３】

$$dk_i = H(u^{a_{0,i}}) \in \{0,1\}^l \quad \cdots (式２００７)$$

【０２６７】

このような手順を経ることにより、鍵処理装置は、鍵処理装置のＤＥＭにおける復号処理に用いられるセッション鍵ｄｋを算出することができる。

【０２６８】

［基盤技術である暗号処理方法の問題点］

上述のような本実施形態に係る情報処理方法の基盤技術となる暗号処理方法では、以下のような問題点がある。すなわち、基盤技術では、暗号化方法において、それぞれの受信者の公開鍵を用いて検証用パラメータ$v_1$，$v_2$，・・・，$v_n$を計算し、暗号文φに挿入している。暗号文の受信者は、復号方法において、式２００６における等号が成立するか否かを検証することにより、不当な暗号文を排除することが可能となっている。しかしながら、この検証方法を実現するために、受信者数をｎとしたときｎ回のｍｕｌｔｉ－ｓｃａｌａｒ　ｍｕｌｔｉｐｌｉｃａｔｉｏｎの処理が暗号化の際に必要となる。さらに、生成される暗号文においても、ｎ＋１個の要素が必要となる。これらの値が大きいという点が、基盤技術における問題点である。

【０２６９】

＜情報処理方法について＞

本実施形態に係る情報処理方法では、上記問題を解決するために、以下の点に着目した。すなわち、基盤技術における暗号化処理では、受信者に固有の二次関数$f_i$（ｘ）を用いて、各受信者用にパラメータの算出を行なっていた。そこで、受信者に固有の二次関数中に何らかの共有情報を存在させることで、暗号化方法を効率よく実行可能である点に想到した。以下に示す本実施形態に係る情報処理方法では、受信者に固有の二次関数のうち、二次関数のｙ切片にあたるパラメータを共通化してシステムパラメータに加えることにより、情報処理方法全体における効率化を実現している。

【０２７０】

以下、本実施形態に係る情報処理方法について、図３２～図３５を参照しながら、詳細に説明する。図３２～図３５は、本実施形態に係る情報処理方法について説明するための流れ図である。

【０２７１】

［システムパラメータ生成方法について］

まず、図３２を参照しながら、本実施形態に係るシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、システムパラメータ生成装置として機能する本実施形態に係る情報処理装置１０において実行される。

【０２７２】

まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ２０１）。

【０２７３】

次に、情報処理装置１０の関数選択部１０３は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0,1\}^1$という写像を実現する関数Ｈと、を選択する（ステップＳ２０２）。

【０２７４】

続いて、情報処理装置１０のパラメータ選択部１０５は、パラメータｇ，$y_0 \in_R G$を選択する（ステップＳ２０３）。

【０２７５】

次に、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩをＩ＝（ｐ，Ｇ，ｇ，$y_0$，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ２０４）。

【０２７６】
このような手順を経ることにより、システムパラメータ生成装置として機能する情報処理装置１０は、鍵処理装置として機能する情報処理装置２０のｍＫＥＭ２０１が暗号処理を実行する際に必要となるシステムパラメータを生成することができる。
【０２７７】
［鍵生成方法について］
次に、図３３を参照しながら、本実施形態に係る鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持し、鍵処理装置として機能する情報処理装置２０の鍵生成部２１１において実行される。なお、この鍵生成方法は、情報処理装置２０を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、情報処理装置２０がシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。
【０２７８】
まず、パラメータ生成部２１３は、情報処理装置２０に固有の秘密情報として、パラメータｓ，ｔ，$F_s$，$F_t \in_R Z_p$を選択し、（ｆ（０），ｆ（ｓ），ｆ（ｔ））＝（$\log_g y_0$，$F_s$，$F_t$）と定義する（ステップＳ２１１）。本実施形態において、このような４種類のパラメータを選択し、ｆ（０），ｆ（ｓ），ｆ（ｔ）を定義するということは、$f(x)=a_0+a_1x+a_2x^2$という二次関数を定義したことと同様の意味を有する。
【０２７９】
次に、パラメータ生成部２１３は、選択したパラメータｆ（０），ｆ（ｓ），ｆ（ｔ）と、システムパラメータであるｇとを用い、ラグランジュの補間公式を利用して、以下の式２０１～式２０２に示すパラメータ$y_1$，$y_2$を算出する（ステップＳ２１２）。
【０２８０】
【数２４】

$$y_1 = g^{a_1} \in G \quad \cdots \text{(式２０１)}$$

$$y_2 = g^{a_2} \in G \cdots \text{(式２０２)}$$

【０２８１】
その後、秘密鍵生成部２１５は、情報処理装置２０を所持するユーザに固有の秘密鍵ｓｋ＝（ｓ，ｔ，$F_s$，$F_t$）を生成する（ステップＳ２１３）。また、公開鍵生成部２１７は、情報処理装置２０を所持するユーザに固有の公開鍵ｐｋ＝（$y_1$，$y_2$）を生成する（ステップＳ２１４）。
【０２８２】
その後、鍵生成部２１１は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ２１５）。また、公開鍵公開部２１９は、生成した公開鍵ｐｋを、他の情報処理装置２０に対して公開する。
【０２８３】
このような手順を経ることにより、情報処理装置２０の鍵生成部２１１は、情報処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。
【０２８４】
［暗号化方法について］
次に、図３４を参照しながら、本実施形態に係る暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持し、鍵処理装置として機能する情報処理装置２０の暗号化部２２１において実行される。なお、この暗号化方法は、情報処理装置２０を所持し、メッセージの送信を行うユーザが、複数受信者ＫＥＭを用いて暗号文を生成する際に実行される。
【０２８５】

まず、パラメータ選択部２２３は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ２２１）。

【０２８６】

次に、パラメータ選択部２２３は、選択したパラメータｒと、システムパラメータとして公開されているパラメータｇとを用いて、パラメータ$u = g^r \in G$を算出する（ステップＳ２２２）。

【０２８７】

続いて、パラメータ選択部２２３は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ２２３）。

【０２８８】

次に、検証用パラメータ生成部２２５は、メッセージの送信を行う情報処理装置２０全てに対して、ラグランジュの補間公式を利用して、検証用パラメータ$v_i$を、以下の式２０３に基づいて算出する（ステップＳ２２４）。以下の式２０３から明らかなように、検証用パラメータｖｉは、送信先の情報処理装置２０の公開鍵$pk_i$（ｉ＝１，・・・ｎ）と、システムパラメータと、パラメータ選択部２２３によって選択されたパラメータと、を用いて、算出可能である。

【０２８９】

【数２５】

$$v_i = y_0^r \cdot y_{1,i}^{r\alpha} \cdot y_{2,i}^{r\alpha^2} \left(= g^{r \cdot f_i(\alpha)}\right) \quad \cdots (式２０３)$$

【０２９０】

続いて、セッション鍵算出部２３７は、メッセージの送信を行う全ての情報処理装置２０に対して、システムパラメータを用いて、以下のセッション鍵ｄｋを算出する（ステップＳ２２５）。

【０２９１】

【数２６】

$$dk = H(y_0^r) \in \{0,1\}^l \quad \cdots (式２０４)$$

【０２９２】

次に、暗号化部２２１は、$\phi = (u, v_1, v_2, \cdots, v_n)$とし、$(\phi, dk)$を出力する（ステップＳ２２６）。

【０２９３】

このような手順を経ることにより、情報処理装置２０は、ＤＥＭ２０３において実行される共通鍵暗号処理に用いられるセッション鍵ｄｋを生成することができる。

【０２９４】

上述のように、基盤技術における暗号化方法では、受信者の公開鍵$pk_i$を用いて各受信者に対してセッション鍵$dk_i$を算出していたが、本実施形態に係る暗号化方法では、システムパラメータとして公開されている値を用いてセッション鍵ｄｋを生成する。これにより、本実施形態に係る暗号化方法では、演算回数の削減を図ることが可能となる。

【０２９５】

［復号方法について］

次に、図３５を参照しながら、本実施形態に係る復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置２０の復号部２３１において実行される。

【０２９６】

復号処理に先立ち、復号部２３１は、暗号文の中に含まれる$\phi = (u, v_1, v_2, \cdots, v_n)$の中から、自身に関係する部分$(u, v_i)$を抽出する。この抽出処理は、記載されている$v_i$の順番とユーザとの対応関係とを関連付けるラベルを用いたり、送信者がそれぞれの受信者に必要な情報だけが届くように設定したりすることで実現可能であ

る。

【０２９７】

まず、パラメータ算出部２３３は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈$Z_p$を算出する（ステップＳ２３１）。

【０２９８】

次に、セッション鍵算出部２３７は、自身の秘密鍵$sk_i$と、算出したパラメータαと、暗号文に含まれるｕ，$v_i$とを用いて、以下の式２０５に基づいて、パラメータｆ’（α），ｆ’（ｓ），ｆ’（ｔ）を定義する（ステップＳ２３２）。

【０２９９】

【数２７】

$$(f'(\alpha), f'(s), f'(t)) = (\log_u v_i, F_s, F_t) \quad \cdots (式２０５)$$

【０３００】

上記式２０５に示したようなパラメータの定義を行なうことは、二次関数ｆ’（ｘ）を定義していることを表している。ここで、$F_s$、$F_t$は、自身で設定した秘密鍵である。ここで、暗号化方法において適式に検証用パラメータ$v_i$が算出されていれば、式２０５により定義される二次関数ｆ’（ｘ）は、鍵生成方法において定義された二次関数ｆ（ｘ）と等しくなる。

【０３０１】

続いて、セッション鍵算出部２３７は、式２０５と、ラグランジュの補間公式とを用いて、パラメータｆ’（０）の値を算出し、以下の式２０６に基づいて、セッション鍵ｄｋを算出する（ステップＳ２３３）。続いて、セッション鍵算出部２３７は、算出したセッション鍵ｄｋを、自装置のＤＥＭ２０３へと出力する（ステップＳ２３４）。

【０３０２】

【数２８】

$$dk = H(u^{f'(0)}) \in \{0,1\}^l \quad \cdots (式２０６)$$

【０３０３】

このような手順を経ることにより、情報処理装置２０の復号部２３１は、ＤＥＭ２０３における復号処理に用いられるセッション鍵ｄｋを算出することができる。

【０３０４】

＜暗号化時の計算量と暗号文のサイズについて＞

以下では、本実施形態に係る情報処理方法の暗号化時における計算量と暗号文のサイズについて、基盤技術における暗号処理方法と比較しながら説明する。

【０３０５】

［暗号化時の計算量について］

まず、受信者数をｎとしたときの、基盤技術における暗号化方法での計算量と、本実施形態に係る暗号化方法での計算量を比較する。両方法ともに、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ、および、ｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が支配的となるため、それぞれの演算数の比較を行った。暗号化時の計算量を比較した結果を、以下の表３に示す。

【０３０６】

【表３】

表３　暗号化時における計算量

| | single-scalar multiplication | multi-scalar multiplication |
|---|---|---|
| 基盤技術 | ｎ＋１ | ｎ |
| 本実施形態 | ２ | ｎ |

【０３０７】
表３より、基盤技術における暗号化方法では、（ｎ＋１）回のｓｉｎｇｌｅ－ｓｃａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。また、本実施形態に係る暗号化方法では、２回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。
【０３０８】
非特許文献５に記載のように、一般的にｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎは、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの１．５倍の処理が必要であると考えられている。このことを考慮すると、基盤技術における暗号化方法では（２．５ｎ＋１）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が必要である。他方、本実施形態に係る暗号化方式では、（１．５ｎ＋２）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量で処理が完了することが分かる。
【０３０９】
［暗号文のサイズについて］
次に、受信者数をｎとしたときの、基盤技術における暗号文サイズと、本実施形態に係る情報処理方法における暗号文サイズとを比較する。両方法とも、暗号文に含まれる要素数およびｍＫＥＭ中に含まれるＤＥＭにより生成される暗号文の数で比較を行った。得られた結果を、以下の表４に示す。
【０３１０】
【表４】
表４　暗号文のサイズ

| | 群の要素数 | ｍＫＥＭ中に含まれるＤＥＭにより生成される暗号文の数 |
|---|---|---|
| 基盤技術 | ｎ＋１ | ｎ |
| 本実施形態 | ｎ＋１ | ０ |

【０３１１】
表４より、基盤技術および本実施形態では、群の要素数はｎ＋１個と変わらないものの、ｍＫＥＭ中に含まれるＤＥＭにより生成される暗号文の数をなくすことが可能となる。この結果から明らかなように、本実施形態に係る情報処理方法では、暗号文のサイズを、削減することができる。
【０３１２】
以上説明したように、本実施形態に係る情報処理装置および情報処理方法では、鍵処理装置として機能する情報処理装置２０におけるｍＫＥＭ２０１として、図１３に示したｍｓＫＥＭを導入することで、複数受信者公開鍵暗号システムを実現している。
【０３１３】
＜第１変形例について＞
本発明の第２の実施形態に係る情報処理装置および情報処理方法では、システムパラメータとして設定されたパラメータ$y_0$を用いて、受信者に共通のセッション鍵ｄｋを算出する場合について説明した。ここで、パラメータ$y_0$を用いて、受信者に共通のセッション鍵ｄｋではなく、受信者に共通の検証用パラメータを算出することも可能である。すなわち、本発明の第２の実施形態に係る情報処理装置２０では、ｍＫＥＭ２０１としてｍｓＫＥＭを導入した場合について説明したが、ｍＫＥＭ２０１としてｍｍＫＥＭを導入することも可能である。以下では、第１変形例として、第２の実施形態に係る情報処理装置２０にｍｍＫＥＭを導入した場合について、詳細に説明する。
【０３１４】

上述のような変形例を実現するためには、本発明の第２の実施形態に係る暗号化方法および復号方法を、以下のように変形する。

【０３１５】

［暗号化方法について］

まず、図３６を参照しながら、本変形例に係る暗号化方法について、詳細に説明する。図３６は、本変形例に係る暗号化方法を説明するための流れ図である。

【０３１６】

まず、パラメータ選択部２２３は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ２２１）。

【０３１７】

次に、パラメータ選択部２２３は、選択したパラメータｒと、システムパラメータとして公開されているパラメータｇとを用いて、パラメータ$u = g^r \in G$を算出する（ステップＳ２２２）。

【０３１８】

続いて、パラメータ選択部２２３は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ２２３）。

【０３１９】

次に、検証用パラメータ生成部２２５は、メッセージの送信を行う全ての情報処理装置２０に対して、システムパラメータを用いて、検証用パラメータ$v_i$を以下の式２１１に基づいて算出する（ステップＳ２４１）。

【０３２０】

【数２９】

$$v = y_0^r \in \{0,1\}^l \quad \cdots (式２１１)$$

【０３２１】

続いて、鍵処理装置は、メッセージの送信を行う全ての情報処理装置２０に対して、ラグランジュの補間公式を利用して、以下の式２１２で表されるセッション鍵$dk_i$を算出する（ステップＳ２４２）。

【０３２２】

【数３０】

$$dk_i = H(y_0^r \cdot y_{1,i}^{r\alpha} \cdot y_{2,i}^{r\alpha^2}) (= H(g^{r \cdot f_i(\alpha)})) \quad \cdots (式２１２)$$

【０３２３】

次に、暗号化部２２１は、φ＝（ｕ，ｖ）とし、（φ，$dk_1$，$dk_2$，・・・，$dk_n$）を出力する（ステップＳ２４３）。

【０３２４】

［復号方法について］

次に、図３７を参照しながら、本変形例に係る復号方法について、詳細に説明する。図３７は、本変形例に係る復号方法を説明するための流れ図である。

【０３２５】

まず、パラメータ算出部２３３は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ２３１）。

【０３２６】

次に、セッション鍵算出部２３７は、自身の秘密鍵$sk_i$と、暗号文に含まれるｕ，ｖと、システムパラメータとを用いて、以下の式２１３に基づいて、パラメータｆ’（０），ｆ’（ｓ），ｆ’（ｔ）を定義する（ステップＳ２４４）。

【０３２７】
【数３１】

$$(f'(0), f'(s), f'(t)) = (\log_u v, F_s, F_t) \quad \cdots (式２１３)$$

【０３２８】
上記式２１３に示したようなパラメータの定義を行なうことは、二次関数ｆ’（ｘ）を定義していることを表している。ここで、式２１３により定義される二次関数ｆ’（ｘ）は、鍵生成方法において定義された二次関数ｆ（ｘ）と等しくなる。
【０３２９】
続いて、セッション鍵算出部２３７は、式２１３と、ラグランジュの補間公式とを用いて、パラメータｆ’（α）の値を算出し、以下の式２１４に基づいて、セッション鍵ｄｋを算出する（ステップＳ２３３）。続いて、セッション鍵算出部２３７は、算出したセッション鍵ｄｋを、自装置のＤＥＭ２０３へと出力する（ステップＳ２３４）。
【０３３０】
【数３２】

$$dk_i = H(u^{f'(\alpha)}) \in \{0,1\}^l \quad \cdots (式２１４)$$

【０３３１】
＜暗号化時の計算量と暗号文のサイズについて＞
以下では、本変形例に係る情報処理方法の暗号化時における計算量と暗号文のサイズについて、基盤技術における暗号処理方法と比較しながら説明する。
【０３３２】
［暗号化時の計算量について］
まず、受信者数をｎとしたときの、基盤技術における暗号化方法での計算量と、本変形例に係る暗号化方法での計算量を比較する。両方法ともに、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ、および、ｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が支配的となるため、それぞれの演算数の比較を行った。暗号化時の計算量を比較した結果を、以下の表５に示す。
【０３３３】
【表５】
表５　暗号化時における計算量

| | single-scalar multiplication | multi-scalar multiplication |
|---|---|---|
| 基盤技術 | ｎ＋１ | ｎ |
| 本変形例 | ２ | ｎ |

【０３３４】
表５より、基盤技術における暗号化方法では、（ｎ＋１）回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。また、本変形例に係る暗号化方法では、２回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。
【０３３５】
非特許文献５に記載のように、一般的にｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎは、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの１．５倍の処理が必要であると考えられている。このことを考慮すると、基盤技術における暗号化方法では（２．５ｎ＋１）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が必要である。他方、本変形例に係る暗号化方式では、（１．５ｎ＋２）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量で処理が完了することが分かる。

【０３３６】
［暗号文のサイズについて］
次に、受信者数をｎとしたときの、基盤技術における暗号文サイズと、本変形例に係る情報処理方法における暗号文サイズとを比較する。両方法とも、暗号文に含まれる要素数で比較を行った。得られた結果を、以下の表６に示す。
【０３３７】
【表６】

表６　暗号文のサイズ

| | 群の要素数 |
|---|---|
| 基盤技術 | ｎ＋１ |
| 本実施形態 | ２ |

【０３３８】
表６より、基盤技術では、群の要素数はｎ＋１個であるのに対し、本変形例では、群の要素数は、受信者数ｎに依存せず、２個となる。この結果から明らかなように、本実施形態に係る情報処理方法では、暗号文のサイズを、受信者数ｎに依存しないように削減することができる。
【０３３９】
（第３の実施形態）
続いて、図３８～図４５を参照しながら、本発明の第３の実施形態に係る情報処理装置および情報処理方法について、詳細に説明する。
【０３４０】
＜情報処理装置の構成について＞
まず、本実施形態に係る情報処理装置の構成について、説明する。本実施形態に係る情報処理装置は、システムパラメータ生成装置として機能する情報処理装置１０と、鍵処理装置として機能する情報処理装置２０とが存在する。
【０３４１】
ここで、本実施形態におけるシステムパラメータ生成装置として機能する情報処理装置１０は、図１４に示した本発明の第１の実施形態に係る情報処理装置１０の構成を有し、各処理部で実行される処理内容のみが異なるものである。そのため、本実施形態に係る情報処理装置１０が備える各処理部の機能については、以下で本実施形態に係る情報処理方法を説明しながら説明するものとする。
【０３４２】
同様に、本実施形態における鍵処理装置として機能する情報処理装置２０は、図１５および図１６に示した本発明の第１の実施形態に係る情報処理装置２０の構成を有し、各処理部で実行される処理内容のみが異なるものである。そのため、本実施形態に係る情報処理装置２０が備える各処理部の機能については、以下で本実施形態に係る情報処理方法を説明しながら説明するものとする。
【０３４３】
＜本実施形態に係る情報処理方法の基盤となる暗号処理方法について＞
続いて、本実施形態に係る情報処理方法について説明するに先立ち、本実施形態に係る情報処理方法の基盤となる暗号処理方法について、図３８～４１を参照しながら、詳細に説明する。図３８～図４１は、本実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。本実施形態に係る情報処理方法の基盤となる暗号処理方法は、非特許文献３に記載の暗号処理方法である。
【０３４４】
［システムパラメータ生成方法について］
まず、図３８を参照しながら、本実施形態に係る情報処理方法の基盤となるシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、シス

テムパラメータ生成者が所持する情報処理装置であるシステムパラメータ生成装置において実行される。

【０３４５】

まず、システムパラメータ生成装置は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ３００１）。

【０３４６】

次に、システムパラメータ生成装置は、$G \rightarrow Z_p$という写像を実現する関数ＴＣＲと、$G \rightarrow \{0,1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ３００２）。

【０３４７】

続いて、システムパラメータ生成装置は、パラメータ$g \in_R G$を選択する（ステップＳ３００３）。

【０３４８】

次に、システムパラメータ生成装置は、システムパラメータＩをＩ＝（ｐ，Ｇ，ｇ，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ３００４）。

【０３４９】

このような手順を経ることにより、システムパラメータ生成装置は、鍵処理装置の複数受信者ＫＥＭが暗号処理を実行する際に必要となるシステムパラメータを生成することができる。

【０３５０】

［鍵生成方法について］

次に、図３９を参照しながら、本実施形態に係る情報処理方法の基盤となる鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この鍵生成方法は、鍵処理装置を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、鍵処理装置がシステムパラメータ生成装置によって生成されたシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。

【０３５１】

まず、鍵処理装置は、鍵処理装置に固有の秘密情報として、パラメータ$x_1$，$x_2$，$y_1$，$y_2 \in_R Z_p$を選択する（ステップＳ３０１１）。

【０３５２】

次に、鍵処理装置は、選択したパラメータ$x_1$，$x_2$，$y_1$，$y_2$と、システムパラメータであるｇとを用い、以下の式３００１～式３００４に示すパラメータ$c_1$，$c_2$，$d_1$，$d_2$を算出する（ステップＳ３０１２）。

【０３５３】

【数３３】

$$c_1 = g^{x_1} \in G \quad \cdots \text{(式３００１)}$$

$$c_2 = g^{x_2} \in G \cdots \text{(式３００２)}$$

$$d_1 = g^{y_1} \in G \quad \cdots \text{(式３００３)}$$

$$d_2 = g^{y_2} \in G \cdots \text{(式３００４)}$$

【０３５４】

その後、鍵処理装置は、鍵処理装置を所持するユーザに固有の秘密鍵ｓｋ＝（$x_1$，$x_2$，$y_1$，$y_2$）を生成する（ステップＳ３０１３）。また、鍵処理装置は、鍵処理装置を所持するユーザに固有の公開鍵ｐｋ＝（$c_1$，$c_2$，$d_1$，$d_2$）を生成する（ステップＳ３０１４）。

【０３５５】
その後、鍵処理装置は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ３０１５）。また、生成した公開鍵ｐｋは、他の鍵処理装置に対して公開される。
【０３５６】
このような手順を経ることにより、鍵処理装置は、鍵処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。
【０３５７】
［暗号化方法について］
次に、図４０を参照しながら、本実施形態に係る情報処理方法の基盤となる暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この暗号化方法は、鍵処理装置を所持し、メッセージの送信を行うユーザが、複数受信者ＫＥＭを用いて暗号文を生成する際に実行される。
【０３５８】
まず、鍵処理装置は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ３０２１）。
【０３５９】
次に、鍵処理装置は、選択したパラメータｒと、システムパラメータとして公開されているパラメータｇとを用いて、パラメータ$u = g^r \in G$を算出する（ステップＳ３０２２）。
【０３６０】
続いて、鍵処理装置は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ３０２３）。
【０３６１】
次に、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵$pk_i$（ｉ＝１，・・・ｎ）を用い、式３００５および式３００６に示した２種類の検証用パラメータ$v_{1,i}, v_{2,i}$を算出する（ステップＳ３０２４）。
【０３６２】
【数３４】

$$v_{1,i} = c_{1,i}^{r\alpha} \cdot d_{1,i}^{r} \in \mathbf{G} \quad \cdots (式３００５)$$

$$v_{2,i} = c_{2,i}^{r\alpha} \cdot d_{2,i}^{r} \in \mathbf{G} \quad \cdots (式３００６)$$

【０３６３】
続いて、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵$pk_i$（ｉ＝１，・・・ｎ）を用いて、以下のセッション鍵$dk_i$を算出する（ステップＳ３０２５）。
【０３６４】
【数３５】

$$dk_i = H(c_{1,i}^{r}) \in \{0,1\}^{l} \quad \cdots (式３００７)$$

【０３６５】
次に、鍵処理装置は、$\phi = (u, v_{1,1}, v_{1,2}, \cdots, v_{1,n}, v_{2,1}, v_{2,2}, \cdots, v_{2,n})$とし、$(\phi, dk_1, dk_2, \cdots, dk_n)$を出力する（ステップＳ３０２６）。
【０３６６】
このような手順を経ることにより、鍵処理装置は、鍵処理装置のＤＥＭにおいて実行さ

れる共通鍵暗号処理に用いられるセッション鍵ｄｋを生成することができる。

【０３６７】

［復号方法について］

次に、図４１を参照しながら、本実施形態に係る情報処理方法の基盤となる復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置である鍵処理装置において実行される。

【０３６８】

復号処理に先立ち、鍵処理装置は、暗号文の中に含まれるφ＝（ｕ，$v_{1,1}$，$v_{1,2}$，・・・，$v_{1,n}$，$v_{2,1}$，$v_{2,2}$，・・・，$v_{2,n}$）の中から、自身に関係する部分（ｕ，$v_{1,i}$，$v_{2,i}$）を抽出する。この抽出処理は、記載されている$v_{1,i}$，$v_{2,i}$の順番とユーザとの対応関係とを関連付けるラベルを用いたり、送信者がそれぞれの受信者に必要な情報だけが届くように設定したりすることで実現可能である。

【０３６９】

まず、鍵処理装置は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈$Z_p$を算出する（ステップＳ３０３１）。

【０３７０】

次に、鍵処理装置は、自身の秘密鍵$sk_i$と、システムパラメータと、算出したパラメータαと、暗号文に含まれるｕ，$v_{1,i}$，$v_{2,i}$とを用いて、暗号文の検証処理を行う。より詳細には、鍵処理装置は、以下の式３００８および式３００９における等号が両方とも成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ３０３２）。

【０３７１】

【数３６】

$$v_{1,i}=u^{x_1\alpha+y_1} \quad \cdots(式３００８)$$

$$v_{2,i}=u^{x_2\alpha+y_2} \quad \cdots(式３００９)$$

【０３７２】

鍵処理装置は、上記式３００８および式３００９の等号が両方とも成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ３０３３）復号処理を終了する。

【０３７３】

また、上記式３００８および式３００９の等号が両方とも成立した場合には、鍵処理装置は、受信した暗号文が正当なものであると判断し、自身の秘密鍵$sk_i$と、暗号文に含まれるパラメータｕと、システムパラメータとを用いて、自身に対応するセッション鍵$dk_i$を、以下の式３０１０を用いて算出する（ステップＳ３０３４）。続いて、鍵処理装置は、算出したセッション鍵$dk_i$を、自装置のＤＥＭへと出力する（ステップＳ３０３５）。

【０３７４】

【数３７】

$$dk_i=H(u^{x_1})\in\{0,1\}^l \quad \cdots(式３０１０)$$

【０３７５】

このような手順を経ることにより、鍵処理装置は、鍵処理装置のＤＥＭにおける復号処理に用いられるセッション鍵$dk_i$を算出することができる。

【０３７６】

［基盤技術である暗号処理方法の問題点］

上述のような本実施形態に係る情報処理方法の基盤技術となる暗号処理方法では、以下のような問題点がある。すなわち、基盤技術では、暗号化方法において、それぞれの受信者の公開鍵を用いて検証用パラメータ$v_{1,1}$，$v_{1,2}$，・・・，$v_{1,n}$，$v_{2,1}$

，$v_{2,2}$，・・・，$v_{2,n}$を計算し、暗号文φに挿入している。暗号文の受信者は、復号方法において、式２００６における等号が成立するか否かを検証することにより、不当な暗号文を排除することが可能となっている。しかしながら、この検証方法を実現するために、受信者数をｎとしたとき２ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの処理が暗号化の際に必要となる。さらに、生成される暗号文においても、２ｎ＋１個の要素が必要となる。これらの値が大きいという点が、基盤技術における問題点である。

【０３７７】

＜情報処理方法について＞

本実施形態に係る情報処理方法では、上記問題を解決するために、セッション鍵の算出に用いられるパラメータの一つを共通化してシステムパラメータに加えることにより、情報処理方法全体における効率化を実現している。

【０３７８】

以下、本実施形態に係る情報処理方法について、図４２～図４５を参照しながら、詳細に説明する。図４２～図４５は、本実施形態に係る情報処理方法について説明するための流れ図である。

【０３７９】

［システムパラメータ生成方法について］

まず、図４２を参照しながら、本実施形態に係るシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、システムパラメータ生成装置として機能する本実施形態に係る情報処理装置１０において実行される。

【０３８０】

まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ３０１）。

【０３８１】

次に、情報処理装置１０の関数選択部１０３は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0, 1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ３０２）。

【０３８２】

続いて、情報処理装置１０のパラメータ選択部１０５は、パラメータ$g, c_1 \in_R G$を選択する（ステップＳ３０３）。

【０３８３】

次に、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩをＩ＝（ｐ，Ｇ，ｇ，$c_1$，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ３０４）。

【０３８４】

このような手順を経ることにより、システムパラメータ生成装置として機能する情報処理装置１０は、鍵処理装置として機能する情報処理装置２０のｍＫＥＭ２０１が暗号処理を実行する際に必要となるシステムパラメータを生成することができる。

【０３８５】

［鍵生成方法について］

次に、図４３を参照しながら、本実施形態に係る鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持し、鍵処理装置として機能する情報処理装置２０の鍵生成部２１１において実行される。なお、この鍵生成方法は、情報処理装置２０を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、情報処理装置２０がシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。

【０３８６】

まず、パラメータ生成部２１３は、情報処理装置２０に固有の秘密情報として、パラメ

ータｓ，ｔ∈$_{R}$Ｚ$_{p}$を選択する（ステップＳ３１１）。

【０３８７】

次に、パラメータ生成部２１３は、選択したパラメータｓ，ｔと、システムパラメータであるｇ，ｃ$_{1}$とを用い、以下の式３０１に示すパラメータｃ$_{2}$を算出する（ステップＳ３１２）。

【０３８８】

【数３８】

$$c_2 = g^s \cdot c_1^{-t} \in \mathbf{G} \quad \cdots (式３０１)$$

【０３８９】

続いて、パラメータ生成部２１３は、情報処理装置２０に固有の秘密情報として、以下の式３０２に示す３種類のパラメータを選択する（ステップＳ３１３）。

【０３９０】

【数３９】

$$w_1, w_2, \bar{\alpha} \in_R \mathbf{Z_p} \quad \cdots (式３０２)$$

【０３９１】

次に、パラメータ生成部２１３は、生成したパラメータと、システムパラメータとを用いて、以下の式３０３および式３０４に示すパラメータｄ$_{1}$，ｄ$_{2}$を生成する（ステップＳ３１４）。

【０３９２】

【数４０】

$$d_1 = c_1^{-\bar{\alpha}} \cdot g^{w_1} \in \mathbf{G} \quad \cdots (式３０３)$$

$$d_2 = c_2^{-\bar{\alpha}} \cdot g^{w_2} \in \mathbf{G} \cdots (式３０４)$$

【０３９３】

その後、秘密鍵生成部２１５は、情報処理装置２０を所持するユーザに固有の秘密鍵ｓｋを、以下の式３０５に基づいて生成する（ステップＳ３１５）。

【０３９４】

【数４１】

$$sk = (s, t, w_1, w_2, \bar{\alpha}) \quad \cdots (式３０５)$$

【０３９５】

また、公開鍵生成部２１７は、情報処理装置２０を所持するユーザに固有の公開鍵ｐｋ＝（ｃ$_{2}$，ｄ$_{1}$，ｄ$_{2}$）を生成する（ステップＳ３１６）。

【０３９６】

その後、鍵生成部２１１は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ３１７）。また、公開鍵公開部２１９は、生成した公開鍵ｐｋを、他の情報処理装置２０に対して公開する。

【０３９７】

このような手順を経ることにより、情報処理装置２０の鍵生成部２１１は、情報処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。

【０３９８】

［暗号化方法について］

次に、図４４を参照しながら、本実施形態に係る暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持し、鍵処理装置として機能する情報処理装置２０の暗号化部２２１において実行される。なお、この暗号化方法は、情報処理装置２０を所持し、メッセージの送信を行うユーザが、複数受信者

ＫＥＭを用いて暗号文を生成する際に実行される。

【０３９９】

まず、パラメータ選択部２２３は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ３２１）。

【０４００】

次に、パラメータ選択部２２３は、選択したパラメータｒと、システムパラメータとして公開されているパラメータｇとを用いて、パラメータ$u = g^r \in G$を算出する（ステップＳ３２２）。

【０４０１】

続いて、パラメータ選択部２２３は、算出したパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータ$\alpha = TCR(u) \in Z_p$を算出する（ステップＳ３２３）。

【０４０２】

次に、検証用パラメータ生成部２２５は、メッセージの送信を行う情報処理装置２０全てに対して、式３０６および式３０７に示した２種類の検証用パラメータ$v_{1,i}$，$v_{2,i}$を算出する（ステップＳ３２４）。以下の式３０６および式３０７から明らかなように、検証用パラメータ$v_{1,i}$，$v_{2,i}$は、送信先の情報処理装置２０の公開鍵$pk_i$（ｉ＝１，・・・ｎ）と、システムパラメータと、選択したパラメータと用いて、算出可能である。

【０４０３】

【数４２】

$$v_{1,i} = c_1^{r\alpha} \cdot d_{1,i}^{r} \in G \quad \cdots(式３０６)$$

$$v_{2,i} = c_{2,i}^{r\alpha} \cdot d_{2,i}^{r} \in G \quad \cdots(式３０７)$$

【０４０４】

続いて、セッション鍵算出部２３７は、メッセージの送信を行う情報処理装置２０全てに対して、システムパラメータと選択したパラメータｒとを用いて、以下のセッション鍵ｄｋを算出する（ステップＳ３２５）。

【０４０５】

【数４３】

$$dk = H(c_1^r) \in \{0,1\}^l \quad \cdots(式３０８)$$

【０４０６】

次に、暗号化部２２１は、$\phi = (u, v_{1,1}, v_{1,2}, \cdots, v_{1,n}, v_{2,1}, v_{2,2}, \cdots, v_{2,n})$とし、（φ，ｄｋ）を出力する（ステップＳ３２６）。

【０４０７】

このような手順を経ることにより、情報処理装置２０は、ＤＥＭ２０３において実行される共通鍵暗号処理に用いられるセッション鍵ｄｋを生成することができる。

【０４０８】

上述のように、基盤技術における暗号化方法では、受信者の公開鍵$pk_i$を用いて各受信者に対してセッション鍵$dk_i$を算出していたが、本実施形態に係る暗号化方法では、システムパラメータとして公開されている値を用いてセッション鍵ｄｋを生成する。これにより、本実施形態に係る暗号化方法では、演算回数の削減を図ることが可能となる。

【０４０９】

［復号方法について］

次に、図４５を参照しながら、本実施形態に係る復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置２０の復号部２３１において実行される

。

【０４１０】

復号処理に先立ち、復号部２３１は、暗号文の中に含まれるφ＝（ｕ，$v_{1,1}$，$v_{1,2}$，・・・，$v_{1,n}$，$v_{2,1}$，$v_{2,2}$，・・・，$v_{2,n}$）の中から、自身に関係する部分（ｕ，$v_{1,i}$，$v_{2,i}$）を抽出する。この抽出処理は、記載されている$v_{1,i}$，$v_{2,i}$の順番とユーザとの対応関係とを関連付けるラベルを用いたり、送信者がそれぞれの受信者に必要な情報だけが届くように設定したりすることで実現可能である。

【０４１１】

まず、パラメータ算出部２３３は、暗号文に含まれるパラメータｕと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（ｕ）∈$Z_p$を算出する（ステップＳ３３１）。

【０４１２】

次に、パラメータ算出部２３３は、自身の秘密鍵$sk_i$と、システムパラメータと、算出したパラメータαと、暗号文に含まれるｕ，$v_{1,i}$，$v_{2,i}$とを用いて、以下の式３０９および式３１０に示した２種類のパラメータを算出する（ステップＳ３３２）。

【０４１３】

【数４４】

$$\bar{v}_1 = \left( v_{1,i} \middle/ u^{w_1} \right)^{1/\alpha-\bar{\alpha}} \in \mathbf{G} \quad \cdots (式３０９)$$

$$\bar{v}_2 = \left( v_{2,i} \middle/ u^{w_2} \right)^{1/\alpha-\bar{\alpha}} \in \mathbf{G} \quad \cdots (式３１０)$$

【０４１４】

続いて、検証部２３５は、自身の秘密鍵$sk_i$と、算出した２種類のパラメータと、暗号文に含まれるｕとを用いて、暗号文の検証処理を行う。より詳細には、検証部２３５は、以下の式３１１における等号が成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ３３３）。

【０４１５】

【数４５】

$$\bar{v}_1^t \cdot \bar{v}_2 = u^s \quad \cdots (式３１１)$$

【０４１６】

検証部２３５は、上記式３１１の等号が成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ３３４）復号処理を終了する。

【０４１７】

また、上記式３１１の等号が成立した場合には、検証部２３５は、受信した暗号文が正当なものであると判断し、暗号文が正当なものである旨を示す情報を、セッション鍵算出部２３７に伝送する。セッション鍵算出部２３７は、システムパラメータと、式３０９に基づいて算出したパラメータとを用いて、セッション鍵ｄｋを、以下の式３１２を用いて算出する（ステップＳ３３５）。続いて、セッション鍵算出部２３７は、算出したセッション鍵ｄｋを、自装置のＤＥＭ２０３へと出力する（ステップＳ３３６）。

【０４１８】

【数４６】

$$dk = H(\bar{v}_1) \in \{0,1\}^l \quad \cdots (式３１２)$$

【０４１９】

このような手順を経ることにより、情報処理装置２０の復号部２３１は、ＤＥＭ２０３における復号処理に用いられるセッション鍵ｄｋを算出することができる。

【０４２０】

＜暗号化時の計算量と暗号文のサイズについて＞

以下では、本実施形態に係る情報処理方法の暗号化時における計算量と暗号文のサイズについて、基盤技術における暗号処理方法と比較しながら説明する。

【０４２１】

［暗号化時の計算量について］

まず、受信者数をｎとしたときの、基盤技術における暗号化方法での計算量と、本実施形態に係る暗号化方法での計算量を比較する。両方法ともに、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎ、および、ｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が支配的となるため、それぞれの演算数の比較を行った。暗号化時の計算量を比較した結果を、以下の表７に示す。

【０４２２】

【表７】

表７　暗号化時における計算量

| | single-scalar multiplication | multi-scalar multiplication |
|---|---|---|
| 基盤技術 | ｎ＋１ | ２ｎ |
| 本実施形態 | ｎ＋３ | ｎ |

【０４２３】

表７より、基盤技術における暗号化方法では、（ｎ＋１）回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、２ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。また、本実施形態に係る暗号化方法では、ｎ＋３回のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎと、ｎ回のｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎが必要であることがわかる。

【０４２４】

非特許文献５に記載のように、一般的にｍｕｌｔｉ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎは、ｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの１．５倍の処理が必要であると考えられている。このことを考慮すると、基盤技術における暗号化方法では（４ｎ＋１）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量が必要である。他方、本実施形態に係る暗号化方式では、（１．５ｎ＋３）回分のｓｉｎｇｌｅ－ｓｃａｌａｒ ｍｕｌｔｉｐｌｉｃａｔｉｏｎの計算量で処理が完了することが分かる。

【０４２５】

［暗号文のサイズについて］

次に、受信者数をｎとしたときの、基盤技術における暗号文サイズと、本実施形態に係る情報処理方法における暗号文サイズとを比較する。両方法とも、暗号文に含まれる要素数およびｍＫＥＭ中に含まれるＤＥＭにより生成される暗号文の数で比較を行った。得られた結果を、以下の表８に示す。

【０４２６】

【表８】

表８　暗号文のサイズ

| | 群の要素数 | ｍＫＥＭ中に含まれるＤＥＭにより生成される暗号文の数 |
|---|---|---|
| 基盤技術 | ２ｎ＋１ | ｎ |
| 本実施形態 | ２ｎ＋１ | ０ |

【０４２７】

表８より、基盤技術および本実施形態では、群の要素数は２ｎ＋１個と変わらないものの、ｍＫＥＭ中に含まれるＤＥＭにより生成される暗号文の数をなくすことが可能となる。この結果から明らかなように、本実施形態に係る情報処理方法では、暗号文のサイズを、削減することができる。

【０４２８】

以上説明したように、本実施形態に係る情報処理装置および情報処理方法では、鍵処理装置として機能する情報処理装置２０におけるｍＫＥＭ２０１として、図１３に示したｍｓＫＥＭを導入することで、複数受信者公開鍵暗号システムを実現している。

【０４２９】

（第４の実施形態）

続いて、図４６～図５６を参照しながら、本発明の第４の実施形態に係る情報処理装置および情報処理方法について、詳細に説明する。

【０４３０】

まず、図４６を参照しながら、本実施形態に係る情報処理装置および情報処理方法が着目している点について、簡単に説明する。

【０４３１】

本発明の各実施形態で着目している複数受信者公開鍵暗号システムでは、システムパラメータが生成した共通のシステムパラメータに基づいて、各ユーザが秘密鍵および公開鍵を生成する。また、各ユーザ間で送信される暗号文は、共通のシステムパラメータと、暗号文の受信者の公開鍵と、に基づいて、生成される。

【０４３２】

ここで、図４６に示したように、悪意のあるシステムパラメータ生成者が、ユーザ間で送信される暗号文の内容を盗み見るために、システムパラメータ中に生成者しか知りえない秘密情報を埋め込んで、各ユーザにシステムパラメータを公開した場合を考える。

【０４３３】

システムに参加している各ユーザは、秘密情報が埋め込まれたシステムパラメータを用いて各自の秘密鍵および公開鍵を生成し、この公開鍵に基づいて暗号文の送信が行なわれる。この場合に、悪意のあるシステムパラメータ生成者は、システムパラメータに埋め込んだ秘密情報に基づいて、暗号文の内容を取得できる可能性がある。

【０４３４】

例えば、システムパラメータとして２種類以上の群の要素が必要な方式において、本来独立して選択するべき群の要素それぞれを独立して選択せずに、これらの要素間に何らかの関連付けを行なって、一つの要素から他の要素を生成するような場合が考えられる。

【０４３５】

そこで、以下に示す本実施形態に係る情報処理装置および情報処理方法では、このようなシステムパラメータへの秘密情報の埋め込みができないように、方式の改良を行なった。

【０４３６】

＜情報処理装置の構成について＞

まず、本実施形態に係る情報処理装置の構成について、説明する。本実施形態に係る情報処理装置は、システムパラメータ生成装置として機能する情報処理装置１０と、鍵処理装置として機能する情報処理装置２０とが存在する。

【０４３７】

ここで、本実施形態におけるシステムパラメータ生成装置として機能する情報処理装置１０は、図１４に示した本発明の第１の実施形態に係る情報処理装置１０の構成を有し、各処理部で実行される処理内容のみが異なるものである。そのため、本実施形態に係る情報処理装置１０が備える各処理部の機能については、以下で本実施形態に係る情報処理方法を説明しながら説明するものとする。

【０４３８】

同様に、本実施形態における鍵処理装置として機能する情報処理装置２０は、図１５お

よび図１６に示した本発明の第１の実施形態に係る情報処理装置２０の構成を有し、各処理部で実行される処理内容のみが異なるものである。そのため、本実施形態に係る情報処理装置２０が備える各処理部の機能については、以下で本実施形態に係る情報処理方法を説明しながら説明するものとする。

【０４３９】

＜本実施形態に係る情報処理方法の基盤となる暗号処理方法について＞

続いて、本実施形態に係る情報処理方法について説明するに先立ち、本実施形態に係る情報処理方法の基盤となる暗号処理方法について、図４７～５０を参照しながら、詳細に説明する。図４７～図５０は、本実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。本実施形態に係る情報処理方法の基盤となる暗号処理方法は、非特許文献４に記載の暗号処理方法である。

【０４４０】

［システムパラメータ生成方法について］

まず、図４７を参照しながら、本実施形態に係る情報処理方法の基盤となるシステムパラメータ生成方法について、詳細に説明する。このシステムパラメータ生成方法は、システムパラメータ生成者が所持する情報処理装置であるシステムパラメータ生成装置において実行される。

【０４４１】

まず、システムパラメータ生成装置は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ４００１）。

【０４４２】

次に、システムパラメータ生成装置は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0, 1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ４００２）。

【０４４３】

続いて、システムパラメータ生成装置は、パラメータ$g_1, g_2 \in_R G$を選択する（ステップＳ４００３）。

【０４４４】

次に、システムパラメータ生成装置は、システムパラメータＩをＩ＝（ｐ，Ｇ，$g_1$，$g_2$，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ４００４）。

【０４４５】

このような手順を経ることにより、システムパラメータ生成装置は、鍵処理装置が暗号処理を実行する際に必要となるシステムパラメータを生成することができる。

【０４４６】

［鍵生成方法について］

次に、図４８を参照しながら、本実施形態に係る情報処理方法の基盤となる鍵生成方法について、詳細に説明する。この鍵生成方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この鍵生成方法は、鍵処理装置を所持するユーザが、自身の公開鍵および秘密鍵を生成する際に実行される。この鍵生成方法は、鍵処理装置がシステムパラメータ生成装置によって生成されたシステムパラメータを取得した後であれば、任意のタイミングで行うことが可能である。

【０４４７】

まず、鍵処理装置は、鍵処理装置に固有の秘密情報として、パラメータ$x_1$，$x_2$，$y_1$，$y_2$，$z \in_R Z_p$を選択する（ステップＳ４０１１）。

【０４４８】

次に、鍵処理装置は、選択したパラメータ$x_1$，$x_2$，$y_1$，$y_2$，ｚと、システムパラメータである$g_1$，$g_2$とを用い、以下の式４００１～式４００３に示すパラメータｃ，ｄ，ｈを算出する（ステップＳ４０１２）。

【０４４９】

【数４７】

$$c = g_1^{x_1} \cdot g_2^{x_2} \quad \cdots (式４００１)$$

$$d = g_1^{y_1} \cdot g_2^{y_2} \quad \cdots (式４００２)$$

$$h = g_1^{z} \quad \cdots (式４００３)$$

【０４５０】

その後、鍵処理装置は、鍵処理装置を所持するユーザに固有の秘密鍵ｓｋ＝（$x_1$，$x_2$，$y_1$，$y_2$，ｚ）を生成する（ステップＳ４０１３）。また、鍵処理装置は、鍵処理装置を所持するユーザに固有の公開鍵ｐｋ＝（ｃ，ｄ，ｈ）を生成する（ステップＳ４０１４）。

【０４５１】

その後、鍵処理装置は、生成した公開鍵ｐｋと秘密鍵ｓｋとをユーザに対して出力する（ステップＳ４０１５）。また、生成した公開鍵ｐｋは、他の鍵処理装置に対して公開される。

【０４５２】

このような手順を経ることにより、鍵処理装置は、鍵処理装置を所持するユーザに固有の鍵である秘密鍵ｓｋおよび公開鍵ｐｋを生成することができる。

【０４５３】

［暗号化方法について］

次に、図４９を参照しながら、本実施形態に係る情報処理方法の基盤となる暗号化方法について、詳細に説明する。この暗号化方法は、複数受信者公開鍵暗号による通信を行うユーザが所持する情報処理装置である鍵処理装置において実行される。なお、この暗号化方法は、鍵処理装置を所持しメッセージの送信を行うユーザが、暗号文を生成する際に実行される。

【０４５４】

まず、鍵処理装置は、パラメータ$r \in_R Z_p$を無作為に選択する（ステップＳ４０２１）。

【０４５５】

次に、鍵処理装置は、選択したパラメータｒと、システムパラメータとして公開されているパラメータ$g_2$とを用いて、パラメータ$u_1 = g_2^{r} \in G$を算出する（ステップＳ４０２２）。

【０４５６】

続いて、鍵処理装置は、送信したいメッセージに対応するデータｍと、システムパラメータとして公開されているパラメータ$g_1$と、選択したパラメータｒとを用いて、暗号文$\chi = m g_1^{r}$を生成する（ステップＳ４０２３）。

【０４５７】

次に、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵$pk_i$（ｉ＝１，・・・ｎ）と選択したパラメータｒとを用いて、パラメータ$u_{2,i} = h_i^{r}$を算出する（ステップＳ４０２４）。

【０４５８】

続いて、鍵処理装置は、算出したパラメータ$u_1$，$u_{2,i}$と、暗号文χと、公開されている関数ＴＣＲとを用いて、メッセージの送信を行う鍵処理装置全てに対して、パラメータα＝ＴＣＲ（$u_1$，$u_{2,i}$，χ）を算出する（ステップＳ４０２５）。

【０４５９】

次に、鍵処理装置は、メッセージの送信を行う鍵処理装置全てに対して、送信先の鍵処理装置の公開鍵$pk_i$（ｉ＝１，・・・ｎ）を用い、式４００４に示した検証用パラメータ$v_i$を算出する（ステップＳ４０２６）。

【０４６０】
【数４８】

$$v_i = c_i^r \cdot d_i^{r\alpha} \quad \cdots (式４００４)$$

【０４６１】
続いて、鍵処理装置は、各鍵処理装置に対して送信するデータとして、（$u_{1}$，$u_{2,1}$，$u_{2,2}$，・・・，$u_{2,n}$，$v_1$，$v_2$，・・・，$v_n$，χ）を出力する（ステップＳ４０２７）。
【０４６２】
このような手順を経ることにより、鍵処理装置は、他の鍵処理装置に対して送信するメッセージｍを暗号化することができる。
【０４６３】
［復号方法について］
次に、図５０を参照しながら、本実施形態に係る情報処理方法の基盤となる復号方法について、詳細に説明する。この復号方法は、暗号文を受信した情報処理装置である鍵処理装置において実行される。
【０４６４】
復号処理に先立ち、鍵処理装置は、暗号文の中に含まれる（$u_{2,1}$，$u_{2,2}$，・・・，$u_{2,n}$，$v_1$，$v_2$，・・・，$v_n$）の中から、自身に関係する部分（$u_{2,i}$，$v_i$）を抽出する。この抽出処理は、記載されている$u_{2,i}$，$v_i$の順番とユーザとの対応関係とを関連付けるラベルを用いたり、送信者がそれぞれの受信者に必要な情報だけが届くように設定したりすることで実現可能である。
【０４６５】
まず、鍵処理装置は、暗号文に含まれるパラメータ$u_{1}$，$u_{2,i}$，χと、システムパラメータとして公開されている関数ＴＣＲとを用いて、パラメータα＝ＴＣＲ（$u_{1}$，$u_{2,i}$，χ）を算出する（ステップＳ４０３１）。
【０４６６】
次に、鍵処理装置は、自身の秘密鍵$sk_i$と、暗号文に含まれる$u_{2,i}$とを用いて、式４００５で表されるパラメータｕ’を算出する（ステップＳ４０３２）。
【０４６７】
【数４９】

$$u' = u_{2,i}^{z_i^{-1}} \quad \cdots (式４００５)$$

【０４６８】
続いて、鍵処理装置は、自身の秘密鍵$sk_i$と、暗号文に含まれる$u_{1}$，$v_i$と、算出したパラメータα，ｕ’とを用いて、暗号文の検証処理を行う。より詳細には、鍵処理装置は、以下の式４００６における等号が成立するか否かに基づいて、暗号文の検証処理を行う（ステップＳ４０３３）。
【０４６９】
【数５０】

$$v_i = u'^{x_{1,i}+y_{1,i}\alpha} \cdot u_1^{x_{2,i}+y_{2,i}\alpha} \quad \cdots (式４００６)$$

【０４７０】
鍵処理装置は、上記式４００６の等号が成立しない場合には、受信した暗号文が不当なものであると判断し、エラーメッセージを出力して（ステップＳ４０３４）復号処理を終了する。
【０４７１】
また、上記式４００６の等号が成立した場合には、鍵処理装置は、受信した暗号文が正

当なものであると判断し、式４００７を用いて新たにｕ’を算出する（ステップＳ４０３５）。続いて、鍵処理装置は、暗号文を復号して、平文ｍを出力する（ステップＳ４０３６）。

【０４７２】

【数５１】

$$u' = \frac{\chi}{u'} \quad \cdots \text{(式４００７)}$$

【０４７３】

このような手順を経ることにより、鍵処理装置は、暗号文を復号して、平文ｍを出力することができる。

【０４７４】

［基盤技術である暗号処理方法の問題点］

ここで、上述のような基盤技術において、悪意あるシステムパラメータ生成者が、システムパラメータ$g_2$を$g_1$とは独立に選択せずに、$g_2 = g_1^w$というシステムパラメータ生成者しか知りえない関係性を用いて、$g_1$から$g_2$を算出した場合を考える。ここで、$g_2$を算出する際に用いられたパラメータｗが、システムパラメータ生成者しか知りえない秘密情報に相当する。

【０４７５】

パラメータ$g_2$とパラメータ$g_1$とが、パラメータｗを用いて秘密裏に関連付けられていると、復号処理における式４００７が、以下の式４００８のように変形できる。そのため、悪意あるシステムパラメータ生成者は、暗号文中に含まれるパラメータと、秘密情報ｗとを用いて、本来通信を行っているユーザ同士のみしか知りえないメッセージの内容を、盗み見ることが可能となってしまう。

【０４７６】

【数５２】

$$u' = \frac{\chi}{u'} = \frac{\chi}{u_1^{w-1}} \quad \cdots \text{(式４００８)}$$

【０４７７】

＜第２の実施形態に係るシステムパラメータ生成方法について＞

また、本発明の第２の実施形態に係るシステムパラメータ生成方法においても、パラメータ$y_0$を選択する際に、先に選択したパラメータｇと、システムパラメータ生成者しか知りえない秘密情報ｗとを用いて、$y_0 = g^w$と設定することが可能である。パラメータｇおよびパラメータ$y_0$が上述のような関係性を有している場合、復号方法の式２０６は、以下の式４００９のように変形できる。そのため、悪意あるシステムパラメータ生成者は、暗号文中に含まれるパラメータと、秘密情報ｗとを用いて、本来通信を行っているユーザ同士のみしか知りえないメッセージの内容を、盗み見ることが可能となってしまう。

【０４７８】

【数５３】

$$dk = H(u^{f'(0)}) = H(u^w) \quad \cdots \text{(式４００９)}$$

【０４７９】

＜情報処理方法について＞

そこで、本実施形態に係る情報処理方法では、上記問題を解決するために、群の中から選ぶ要素を順に選択するように設定し、選択した要素を、以下で説明するような関数Ｔに入力して、関数Ｔの出力を次の要素の候補として採用するようにした。これにより、出力されるパラメータと、入力したパラメータとに関係する群構造を把握することが困難となる。また、このような関数をシステムパラメータとしてあわせて公開することにより、システムに参加する各ユーザは、適式にパラメータが選択されているかを検証可能なように

した。

【０４８０】

［本実施形態に係る基盤技術の問題点を解決可能な方法について］

まず、非特許文献４に記載の方法における問題点を解決することが可能な本実施形態に係る情報処理方法（より詳細には、システムパラメータ生成方法）について、図５１を参照しながら詳細に説明する。

【０４８１】

まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ４０１）。

【０４８２】

次に、情報処理装置１０の関数選択部１０３は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0, 1\}^1$という写像を実現する関数Ｈと、を選択する（ステップＳ４０２）。

【０４８３】

続いて、情報処理装置１０のパラメータ選択部１０５は、パラメータ$g_1 \in_R G$を選択する（ステップＳ４０３）。

【０４８４】

次に、情報処理装置１０の関数選択部１０３は、関数Ｔを選択し、パラメータ選択部１０５は、パラメータ$g_2 = T(g_1)$と設定する（ステップＳ４０４）。

【０４８５】

続いて、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩを$I = (p, G, g_1, g_2, TCR, H, T)$のように構成し、各鍵処理装置に公開する（ステップＳ４０５）。

【０４８６】

ここで、パラメータ$g_2$を算出する際に用いられる関数Ｔとして、例えば以下のような関数を用いることが可能である。

【０４８７】

用いられる関数Ｔは、例えば、その関数に入力された要素と、関数から出力された要素とを得たとしても、入力された要素から群演算のみを利用して出力された要素を構成することが困難となるような性質を有している。

【０４８８】

ここで、ｐ，ｑを$p = 2q + 1$が成り立つ素数とする。このとき、$Z_p$の中に位数がｑの部分群$G_q$が存在する。この部分群を、群選択部１０１が選択した群Ｇと定める。ここで、素数ｐを例えば１０２４－ｂｉｔであると想定する。

【０４８９】

このとき、例えば図５２に示したように、一つ目のシステムパラメータ$g_1$が選ばれた後、パラメータ$g_1$の上位数ｂｉｔを擬似乱数生成器（ＰＲＮＧ）に入力し、出力された１０２４－ｂｉｔをもう一つの要素$g_2$の候補とする。パラメータ$g_2$の候補がｐを越えておらず、かつ、$Z_p$でｑ乗した値が１となるときは、パラメータ$g_2$の候補をそのままパラメータ$g_2$とする。また、上述の条件を満たさない場合には、パラメータ$g_1$の選択からやり直すこととする。

【０４９０】

上述のような処理を行う関数Ｔを用いることにより、パラメータ$g_1$とパラメータ$g_2$との間にある群構造の関係を推測することが困難となる。

【０４９１】

また、上述のような関数Ｔは、楕円曲線上の有理点の部分集合として構成される素数位数の群に対しても、設定することが可能である。このような素数位数の群に対して、任意の素体からその群に写像するｍａｐ　ｔｏ　ｐｏｉｎｔという関数が知られている。この関数を用いることで、システムパラメータの要素同士の間にある群構造の関係を分からな

くすることが可能である。
【０４９２】
例えば、素数ｐ，ｑ（｜ｐ｜＝１６０，ｐ＝２ｍｏｄ３，ｐ＝ｓｑ＋１）に対して、楕円曲線：$y^2=x^3+1$ ｏｖｅｒ Ｆｐを考える。システムパラメータの一つ目の要素を$g_1$としたとき、関数Ｔを、例えば図５３に示したような処理を実現する処理部と設定することができる。すなわち、パラメータ$g_1$の上位数ビットを擬似乱数生成器にｓｅｅｄとして入力し、出力された例えば１６０－ｂｉｔを$Z_p$の要素$y_0$とする。次に、$x_0=(y_0^2-1)^{1/3}\in Z_p$とする。次に$Q_0=(x_0, y_0)$を楕円曲線上の点とし、ｓスカラー倍した点を$g_2$とし、二つ目のシステムパラメータとして出力する。
【０４９３】
このような関数Ｔを１種類のみ使用して、$g_2=T(g_1)$、$g_3=T(g_2)$・・・のように、関数の出力を次のパラメータを算出する際の入力として順に使用することで、複数のパラメータを選択することが可能である。また、このような関数Ｔを複数種類使用して、パラメータ$g_2$をある関数$T_1$を用いて算出したら、パラメータ$g_3$をある関数$T_2$を用いて算出する・・・のようにして、複数のパラメータを選択してもよい。
【０４９４】
また、上述のような関数Ｔの代わりに、既存のハッシュ関数を用いることも可能である。
【０４９５】
［本実施形態に係る基盤技術の問題点を解決可能な方法について］
続いて、本発明の第２の実施形態に記載の方法を改良した情報処理方法（より詳細には、システムパラメータ生成方法）について、図５４を参照しながら詳細に説明する。
【０４９６】
まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ４１１）。
【０４９７】
次に、情報処理装置１０の関数選択部１０３は、$G\to Z_p$という写像を実現する関数ＴＣＲと、$G\to\{0,1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ４１２）。
【０４９８】
続いて、情報処理装置１０のパラメータ選択部１０５は、パラメータ$g\in_R G$を選択する（ステップＳ４１３）。
【０４９９】
次に、情報処理装置１０の関数選択部１０３は、関数Ｔを選択し、パラメータ選択部１０５は、パラメータ$y_0=T(g)$と設定する（ステップＳ４１４）。
【０５００】
続いて、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩを$I=(p, G, g, y_0, TCR, H, T)$のように構成し、各鍵処理装置に公開する（ステップＳ４１５）。
【０５０１】
以上説明したように、システムパラメータの要素を決定する際に、上述のような関数Ｔを用いることにより、悪意あるシステムパラメータ生成者が、ユーザ間で伝送された暗号文の内容を盗み見ることを防止することが可能となる。
【０５０２】
＜第１変形例について＞
上述の説明では、悪意あるシステムパラメータ生成者が、ユーザ間で伝送されている暗号文の内容を盗み見る場合について説明した。ここで、例えば、暗号システムの設計者や会社の上司など、ある特別の権力を有する者のみがユーザ間で伝送されている全ての暗号文の内容を復号できるようにシステムパラメータを設定すると、便利である場合が多い。

そこで、本実施形態の第１変形例では、システムパラメータ生成者が、全ての暗号文の内容を復号できるような方式（いわゆるｋｅｙ　ｅｓｃｒｏｗ方式）について、図５５および図５６を参照しながら詳細に説明する。

【０５０３】

［本実施形態に係る基盤技術を改良した情報処理方法について］

まず、本実施形態に係る基盤技術を改良した情報処理方法について、図５５を参照しながら詳細に説明する。本方法は、システムパラメータとして選択されるパラメータ$g_1$とパラメータ$g_2$との間に特別な関係性を持たせることにより、システムパラメータ生成者が、全ての暗号文を復号可能なようにした方法である。

【０５０４】

まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ４２１）。

【０５０５】

次に、情報処理装置１０の関数選択部１０３は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0,1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ４２２）。

【０５０６】

続いて、情報処理装置１０のパラメータ選択部１０５は、パラメータ$g_1 \in_R G$を選択する（ステップＳ４０３）。

【０５０７】

次に、情報処理装置１０のパラメータ選択部１０５は、パラメータｗを選択して、パラメータ$g_2 = g_1^w$と設定する（ステップＳ４２４）。

【０５０８】

続いて、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩをＩ＝（ｐ，Ｇ，$g_1$，$g_2$，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ４２５）。

【０５０９】

パラメータ$g_2$とパラメータ$g_1$とが、パラメータｗを用いて関連付けられていることで、上述のように、復号処理における式４００７が式４００８のように変形できる。そのため、特別な権限を有するシステムパラメータ生成者は、暗号文中に含まれるパラメータと、パラメータｗとを用いて、全ての暗号文を復号することが可能となる。

【０５１０】

［本発明の第２の実施形態に係る方法を改良した情報処理方法について］

次に、本発明の第２の実施形態に係る方法を改良した情報処理方法について、図５６を参照しながら詳細に説明する。本方法は、システムパラメータとして選択されるパラメータｇとパラメータ$y_0$との間に特別な関係性を持たせることにより、システムパラメータ生成者が、全ての暗号文を復号可能なようにした方法である。

【０５１１】

まず、情報処理装置１０の群選択部１０１は、入力されたセキュリティパラメータに基づいて、ｋビットの素数ｐを選択し、ｐを位数とする群Ｇを選択する（ステップＳ４３１）。

【０５１２】

次に、情報処理装置１０の関数選択部１０３は、$G \to Z_p$という写像を実現する関数ＴＣＲと、$G \to \{0,1\}^l$という写像を実現する関数Ｈと、を選択する（ステップＳ４３２）。

【０５１３】

続いて、情報処理装置１０のパラメータ選択部１０５は、パラメータ$g \in_R G$を選択する（ステップＳ４３３）。

【０５１４】

次に、情報処理装置１０のパラメータ選択部１０５は、パラメータwを選択して、パラメータ$y_0 = g^w$と設定する（ステップＳ４３４）。

【０５１５】

続いて、情報処理装置１０のシステムパラメータ生成部１０７は、システムパラメータＩをＩ＝（ｐ，Ｇ，ｇ，$y_0$，ＴＣＲ，Ｈ）のように構成し、各鍵処理装置に公開する（ステップＳ４３５）。

【０５１６】

パラメータｇおよびパラメータ$y_0$がパラメータwを用いて関連付けられていることで、上述のように、復号方法における式２０６は式４００９のように変形できる。そのため、特別な権限を有するシステムパラメータ生成者は、暗号文中に含まれるパラメータと、パラメータwとを用いて、全ての暗号文を復号することが可能となる。

【０５１７】

また、全ての暗号文を復号可能なように所定の関係性が導入されたシステムパラメータと、全ての暗号文を復号できないように所定の関数Ｔを導入したシステムパラメータとを双方公開することも可能である。このように２種類のシステムパラメータを公開することで、メッセージの送信者は、ｋｅｙ　ｅｓｃｒｏｗ方式を利用するかしないかを選択することが可能となる。

【０５１８】

＜ハードウェア構成について＞

次に、図５７を参照しながら、本発明の各実施形態に係る情報処理装置１０のハードウェア構成について、詳細に説明する。図５７は、本発明の各実施形態に係る情報処理装置１０のハードウェア構成を説明するためのブロック図である。

【０５１９】

情報処理装置１０は、主に、ＣＰＵ９０１と、ＲＯＭ９０３と、ＲＡＭ９０５と、を備える。また、情報処理装置１０は、更に、ホストバス９０７と、ブリッジ９０９と、外部バス９１１と、インターフェース９１３と、入力装置９１５と、出力装置９１７と、ストレージ装置９１９と、ドライブ９２１と、接続ポート９２３と、通信装置９２５とを備える。

【０５２０】

ＣＰＵ９０１は、演算処理装置および制御装置として機能し、ＲＯＭ９０３、ＲＡＭ９０５、ストレージ装置９１９、またはリムーバブル記録媒体９２７に記録された各種プログラムに従って、情報処理装置１０内の動作全般またはその一部を制御する。ＲＯＭ９０３は、ＣＰＵ９０１が使用するプログラムや演算パラメータ等を記憶する。ＲＡＭ９０５は、ＣＰＵ９０１の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を一次記憶する。これらはＣＰＵバス等の内部バスにより構成されるホストバス９０７により相互に接続されている。

【０５２１】

ホストバス９０７は、ブリッジ９０９を介して、ＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ　Ｃｏｍｐｏｎｅｎｔ　Ｉｎｔｅｒｃｏｎｎｅｃｔ／Ｉｎｔｅｒｆａｃｅ）バスなどの外部バス９１１に接続されている。

【０５２２】

入力装置９１５は、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチおよびレバーなどユーザが操作する操作手段である。また、入力装置９１５は、例えば、赤外線やその他の電波を利用したリモートコントロール手段（いわゆる、リモコン）であってもよいし、情報処理装置１０の操作に対応した携帯電話やＰＤＡ等の外部接続機器９２９であってもよい。さらに、入力装置９１５は、例えば、上記の操作手段を用いてユーザにより入力された情報に基づいて入力信号を生成し、ＣＰＵ９０１に出力する入力制御回路などから構成されている。情報処理装置１０のユーザは、この入力装置９１５を操作することにより、情報処理装置１０に対して各種のデータを入力したり処理動作を指示したりすることができる。

【０５２３】
出力装置９１７は、取得した情報をユーザに対して視覚的または聴覚的に通知することが可能な装置で構成される。このような装置として、ＣＲＴディスプレイ装置、液晶ディスプレイ装置、プラズマディスプレイ装置、ＥＬディスプレイ装置およびランプなどの表示装置や、スピーカおよびヘッドホンなどの音声出力装置や、プリンタ装置、携帯電話、ファクシミリなどがある。出力装置９１７は、例えば、情報処理装置１０が行った各種処理により得られた結果を出力する。具体的には、表示装置は、情報処理装置１０が行った各種処理により得られた結果を、テキストまたはイメージで表示する。他方、音声出力装置は、再生された音声データや音響データ等からなるオーディオ信号をアナログ信号に変換して出力する。

【０５２４】
ストレージ装置９１９は、情報処理装置１０の記憶部の一例として構成されたデータ格納用の装置である。ストレージ装置９１９は、例えば、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）等の磁気記憶部デバイス、半導体記憶デバイス、光記憶デバイス、または光磁気記憶デバイス等により構成される。このストレージ装置９１９は、ＣＰＵ９０１が実行するプログラムや各種データ、および外部から取得した各種のデータなどを格納する。

【０５２５】
ドライブ９２１は、記録媒体用リーダライタであり、情報処理装置１０に内蔵、あるいは外付けされる。ドライブ９２１は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記録媒体９２７に記録されている情報を読み出して、ＲＡＭ９０５に出力する。また、ドライブ９２１は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記録媒体９２７に記録を書き込むことも可能である。リムーバブル記録媒体９２７は、例えば、ＤＶＤメディア、ＨＤ－ＤＶＤメディア、Ｂｌｕ－ｒａｙメディア等である。また、リムーバブル記録媒体９２７は、コンパクトフラッシュ（登録商標）（ＣｏｍｐａｃｔＦｌａｓｈ：ＣＦ）、メモリースティック、または、ＳＤメモリカード（Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ ｍｅｍｏｒｙ ｃａｒｄ）等であってもよい。また、リムーバブル記録媒体９２７は、例えば、非接触型ＩＣチップを搭載したＩＣカード（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ ｃａｒｄ）または電子機器等であってもよい。

【０５２６】
接続ポート９２３は、機器を情報処理装置１０に直接接続するためのポートである。接続ポート９２３の一例として、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）ポート、ｉ．Ｌｉｎｋ等のＩＥＥＥ１３９４ポート、ＳＣＳＩ（Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍ Ｉｎｔｅｒｆａｃｅ）ポート等がある。接続ポート９２３の別の例として、ＲＳ－２３２Ｃポート、光オーディオ端子、ＨＤＭＩ（Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ）ポート等がある。この接続ポート９２３に外部接続機器９２９を接続することで、情報処理装置１０は、外部接続機器９２９から直接各種のデータを取得したり、外部接続機器９２９に各種のデータを提供したりする。

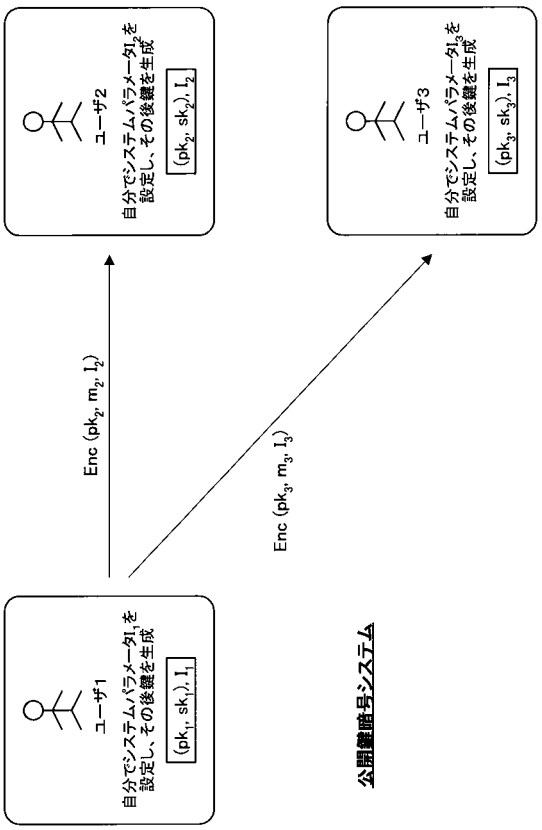
【０５２７】
通信装置９２５は、例えば、通信網９３１に接続するための通信デバイス等で構成された通信インターフェースである。通信装置９２５は、例えば、有線または無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、Ｂｌｕｅｔｏｏｔｈ、またはＷＵＳＢ（Ｗｉｒｅｌｅｓｓ ＵＳＢ）用の通信カード等である。また、通信装置９２５は、光通信用のルータ、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ Ｄｉｇｉｔａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｌｉｎｅ）用のルータ、または、各種通信用のモデム等であってもよい。この通信装置９２５は、例えば、インターネットや他の通信機器との間で、例えばＴＣＰ／ＩＰ等の所定のプロトコルに則して信号等を送受信することができる。また、通信装置９２５に接続される通信網９３１は、有線または無線によって接続されたネットワーク等により構成され、例えば、インターネット、家庭内ＬＡＮ、赤外線通信、ラジオ波通信または衛星通信等であ

ってもよい。
【０５２８】
以上、本発明の各実施形態に係る情報処理装置１０の機能を実現可能なハードウェア構成の一例を示した。上記の各構成要素は、汎用的な部材を用いて構成されていてもよいし、各構成要素の機能に特化したハードウェアにより構成されていてもよい。従って、本実施形態を実施する時々の技術レベルに応じて、適宜、利用するハードウェア構成を変更することが可能である。
【０５２９】
また、本発明の各実施形態に係る情報処理装置２０のハードウェア構成は、本発明の各実施形態に係る情報処理装置１０のハードウェア構成と同様の構成を有しているため、詳細な説明は省略する。
【０５３０】
＜まとめ＞
以上説明したように、本発明の各実施形態に係る情報処理装置および情報処理方法では、各ユーザが共通して使用するシステムパラメータの中に、暗号化処理および復号処理で用いられ、ユーザ固有の秘密情報を含まないパラメータを追加する。これにより、暗号化処理に要する計算量を削減することが可能となり、さらに、暗号文サイズを削減することが可能となる。
【０５３１】
以上、添付図面を参照しながら本発明の好適な実施形態について説明したが、本発明はかかる例に限定されないことは言うまでもない。当業者であれば、特許請求の範囲に記載された範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。
【図面の簡単な説明】
【０５３２】
【図１】公開鍵暗号システムについて説明するための説明図である。
【図２】公開鍵暗号システムについて説明するための説明図である。
【図３】公開鍵暗号システムについて説明するための説明図である。
【図４】複数受信者公開鍵暗号システムについて説明するための説明図である。
【図５】複数受信者公開鍵暗号システムについて説明するための説明図である。
【図６】複数受信者公開鍵暗号システムについて説明するための説明図である。
【図７】複数受信者公開鍵暗号システムについて説明するための説明図である。
【図８】ハイブリッド暗号について説明するための説明図である。
【図９】ハイブリッド暗号について説明するための説明図である。
【図１０】ハイブリッド暗号について説明するための説明図である。
【図１１】ハイブリッド暗号について説明するための説明図である。
【図１２】ハイブリッド暗号について説明するための説明図である。
【図１３】ハイブリッド暗号について説明するための説明図である。
【図１４】本発明の第１の実施形態に係る情報処理装置の構成を説明するためのブロック図である。
【図１５】本発明の第１の実施形態に係る情報処理装置の構成を説明するためのブロック図である。
【図１６】同実施形態に係る情報処理装置の構成を説明するためのブロック図である。
【図１７】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図１８】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図１９】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図２０】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するた

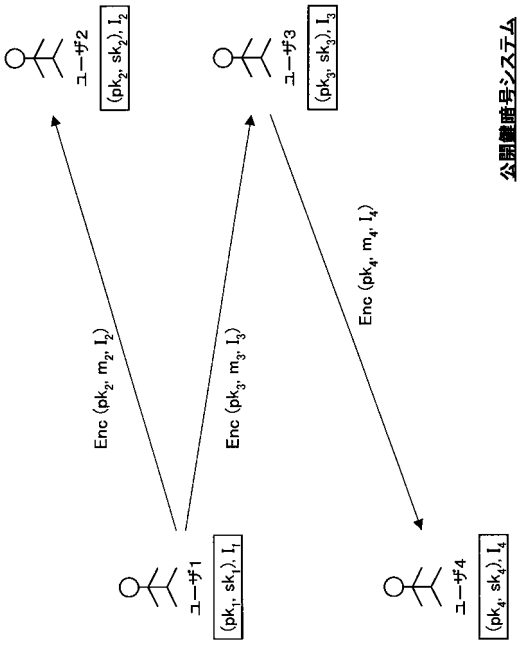
めの流れ図である。
【図２１】同実施形態に係る情報処理方法について説明するための流れ図である。
【図２２】同実施形態に係る情報処理方法について説明するための流れ図である。
【図２３】同実施形態に係る情報処理方法について説明するための流れ図である。
【図２４】同実施形態に係る情報処理方法について説明するための流れ図である。
【図２５】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図２６】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図２７】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図２８】本発明の第２の実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図２９】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図３０】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図３１】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図３２】同実施形態に係る情報処理方法について説明するための流れ図である。
【図３３】同実施形態に係る情報処理方法について説明するための流れ図である。
【図３４】同実施形態に係る情報処理方法について説明するための流れ図である。
【図３５】同実施形態に係る情報処理方法について説明するための流れ図である。
【図３６】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図３７】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図３８】本発明の第３の実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図３９】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図４０】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図４１】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図４２】同実施形態に係る情報処理方法について説明するための流れ図である。
【図４３】同実施形態に係る情報処理方法について説明するための流れ図である。
【図４４】同実施形態に係る情報処理方法について説明するための流れ図である。
【図４５】同実施形態に係る情報処理方法について説明するための流れ図である。
【図４６】本発明の第４の実施形態に係る情報処理方法が着目している点について説明するための説明図である。
【図４７】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図４８】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図４９】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図５０】同実施形態に係る情報処理方法の基盤となる暗号処理方法について説明するための流れ図である。
【図５１】同実施形態に係る情報処理方法について説明するための流れ図である。

【図５２】同実施形態に係る情報処理方法について説明するための説明図である。
【図５３】同実施形態に係る情報処理方法について説明するための説明図である。
【図５４】同実施形態に係る情報処理方法について説明するための説明図である。
【図５５】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図５６】同実施形態に係る情報処理方法の第１変形例について説明するための流れ図である。
【図５７】本発明の各実施形態に係る情報処理装置のハードウェア構成を説明するためのブロック図である。
【符号の説明】
【０５３３】
３　通信網
１０　情報処理装置（システムパラメータ生成装置）
２０　情報処理装置（鍵処理装置）
１０１　群選択部
１０３　関数選択部
１０５　パラメータ選択部
１０７　システムパラメータ生成部
１０９　システムパラメータ公開部
１１１　通信制御部
１１３　記憶部
２０１　ｍＫＥＭ
２０３　ＤＥＭ
２０５　通信制御部
２０７　記憶部
２１１　鍵生成部
２１３　パラメータ生成部
２１５　秘密鍵生成部
２１７　公開鍵生成部
２１９　公開鍵公開部
２２１　暗号化部
２２３　パラメータ選択部
２２５　検証用パラメータ生成部
２２７　セッション鍵生成部
２３１　復号部
２３３　パラメータ算出部
２３５　検証部
２３７　セッション鍵算出部

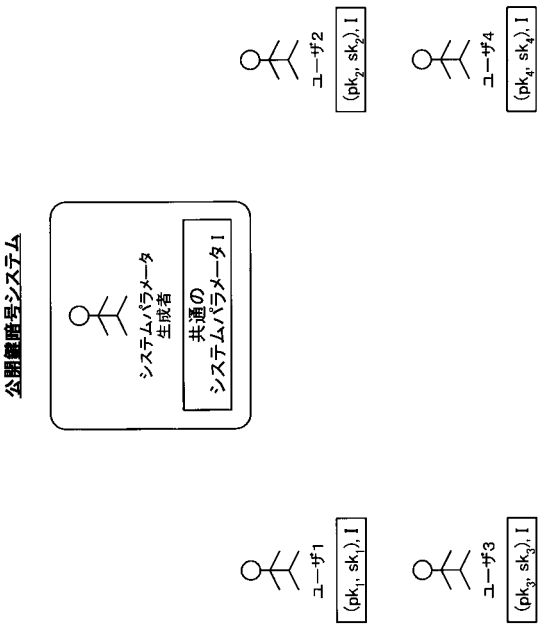
【図１】


ユーザ1
自分でシステムパラメータ$I_1$を設定し、その後鍵を生成
$(pk_1, sk_1), I_1$
ユーザ2
自分でシステムパラメータ$I_2$を設定し、その後鍵を生成
$(pk_2, sk_2), I_2$
ユーザ3
自分でシステムパラメータ$I_3$を設定し、その後鍵を生成
$(pk_3, sk_3), I_3$
Enc $(pk_2, m_2, I_2)$
Enc $(pk_3, m_3, I_3)$
公開鍵暗号システム

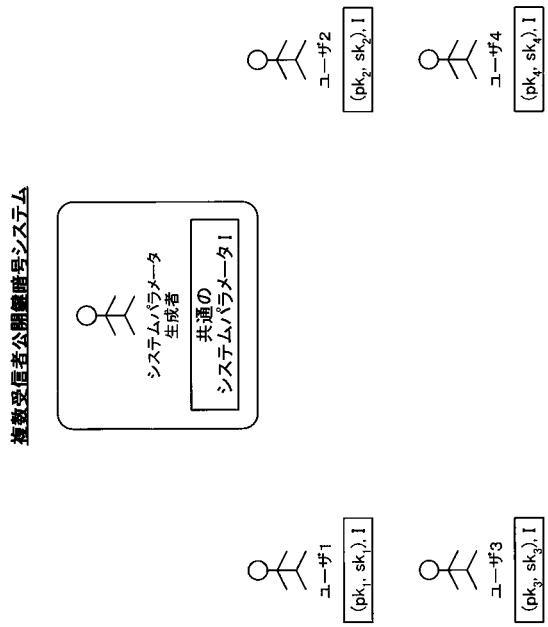
【図２】


ユーザ1
$(pk_1, sk_1), I_1$
ユーザ2
$(pk_2, sk_2), I_2$
ユーザ3
$(pk_3, sk_3), I_3$
ユーザ4
$(pk_4, sk_4), I_4$
Enc $(pk_2, m_2, I_2)$
Enc $(pk_3, m_3, I_3)$
Enc $(pk_4, m_4, I_4)$
公開鍵暗号システム

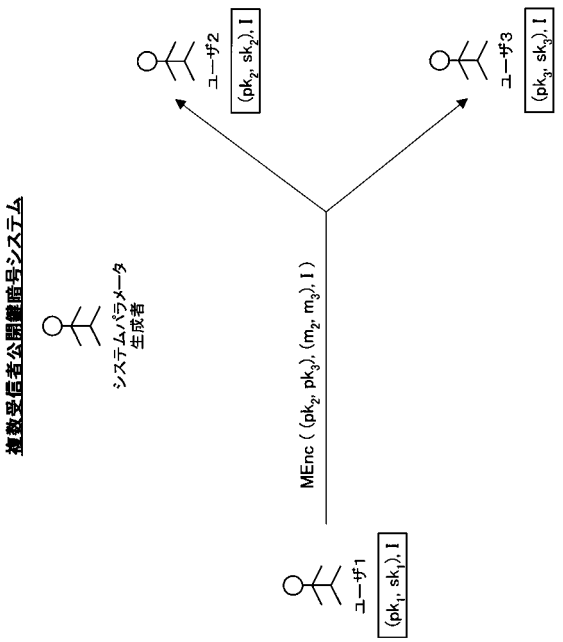
【図３】


公開鍵暗号システム
システムパラメータ生成者
共通のシステムパラメータ I
ユーザ1
$(pk_1, sk_1), I$
ユーザ2
$(pk_2, sk_2), I$
ユーザ3
$(pk_3, sk_3), I$
ユーザ4
$(pk_4, sk_4), I$

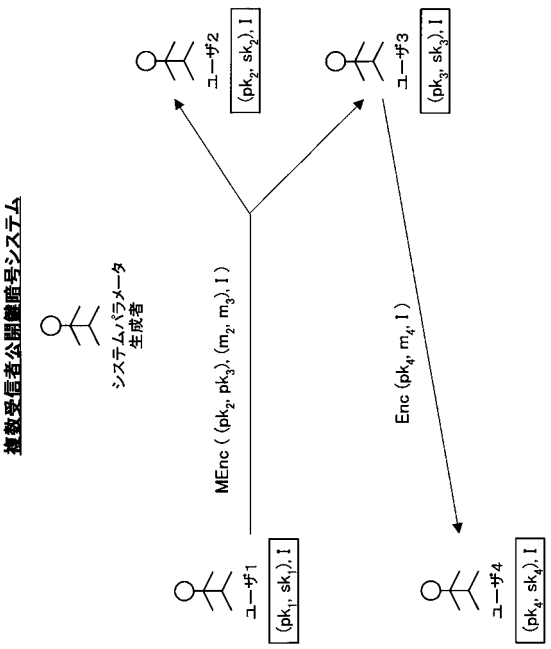
【図４】


複数受信者公開鍵暗号システム
システムパラメータ生成者
共通のシステムパラメータ I
ユーザ1
$(pk_1, sk_1), I$
ユーザ2
$(pk_2, sk_2), I$
ユーザ3
$(pk_3, sk_3), I$
ユーザ4
$(pk_4, sk_4), I$

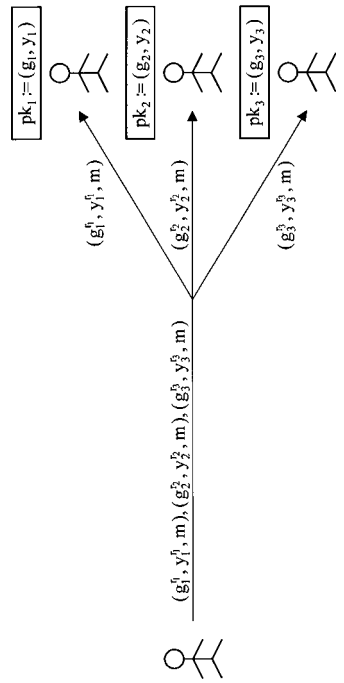
【図５】


複数受信者公開鍵暗号システム
システムパラメータ生成者
MEnc ( (pk2, pk3), (m2, m3), I )
ユーザ1
(pk1, sk1), I
ユーザ2
(pk2, sk2), I
ユーザ3
(pk3, sk3), I

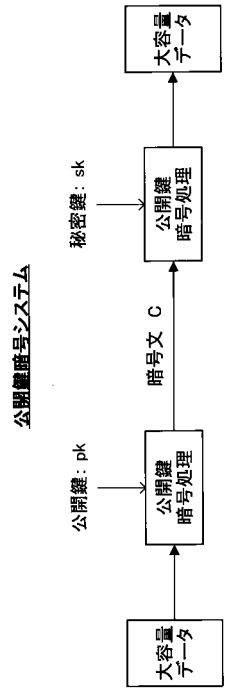
【図６】


複数受信者公開鍵暗号システム
システムパラメータ生成者
MEnc ( (pk2, pk3), (m2, m3), I )
Enc (pk4, m4, I )
ユーザ1
(pk1, sk1), I
ユーザ2
(pk2, sk2), I
ユーザ3
(pk3, sk3), I
ユーザ4
(pk4, sk4), I

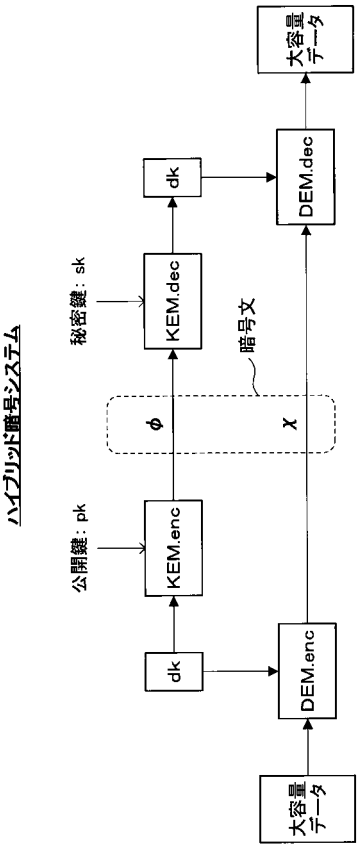
【図７】


pk1 := (g1, y1)
pk2 := (g2, y2)
pk3 := (g3, y3)
(g1r, y1r, m)
(g2r, y2r, m)
(g3r, y3r, m)
(g1r, y1r, m), (g2r, y2r, m), (g3r, y3r, m)

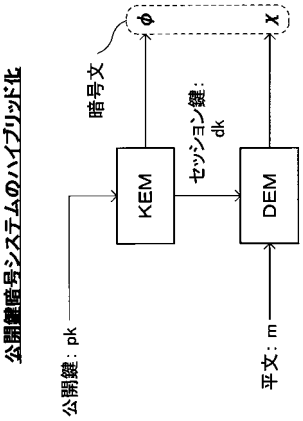
【図８】


公開鍵暗号システム
大容量データ
公開鍵 : pk
公開鍵暗号処理
暗号文 C
秘密鍵 : sk
公開鍵暗号処理
大容量データ

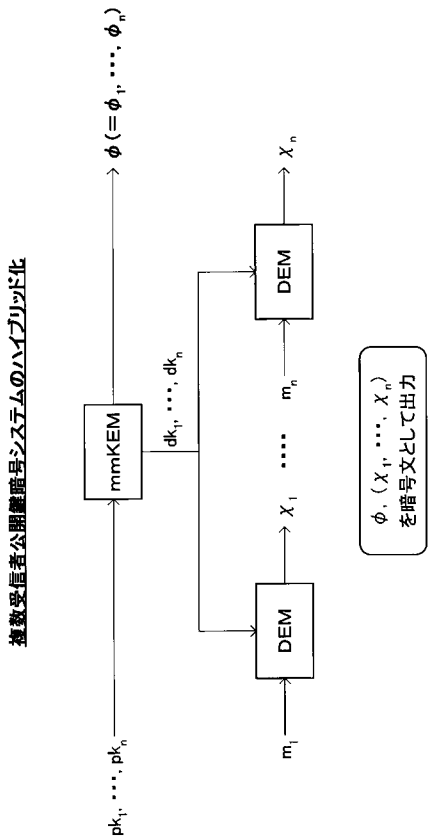
【図９】



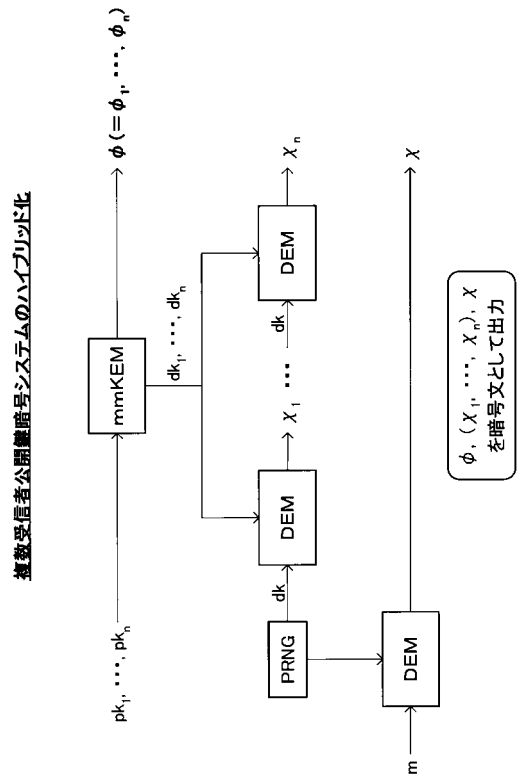

【図１０】



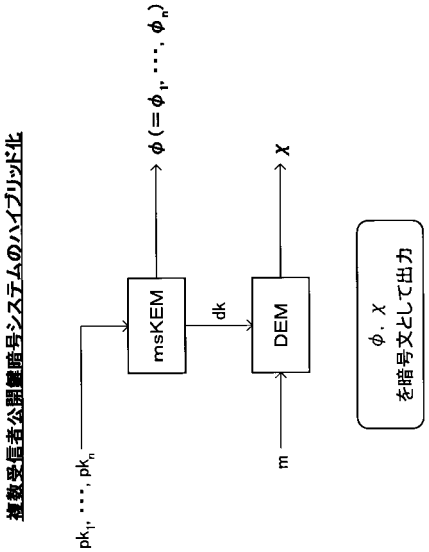

【図１１】



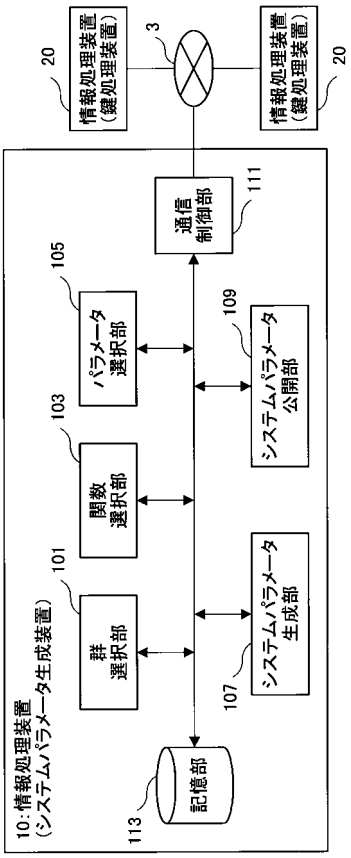

【図１２】



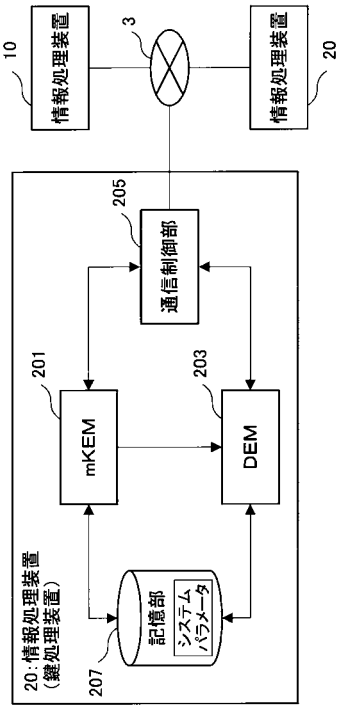
【図１３】



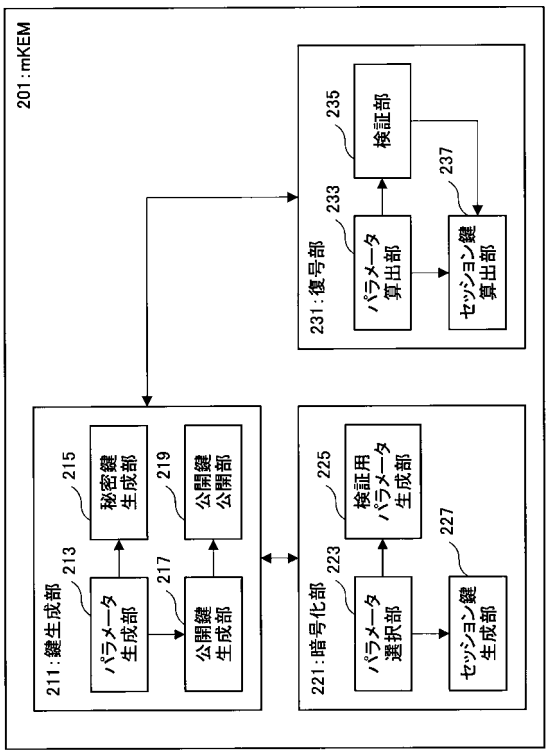

【図１４】



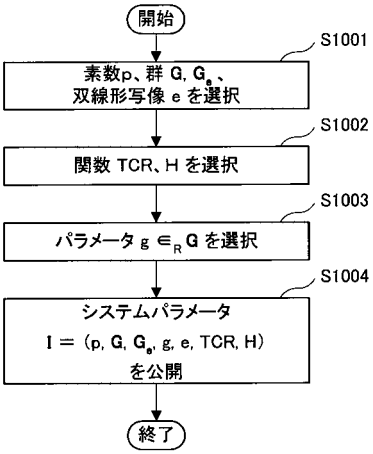

【図１５】



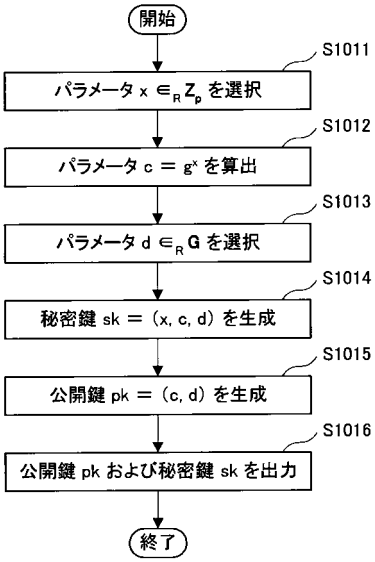

【図１６】



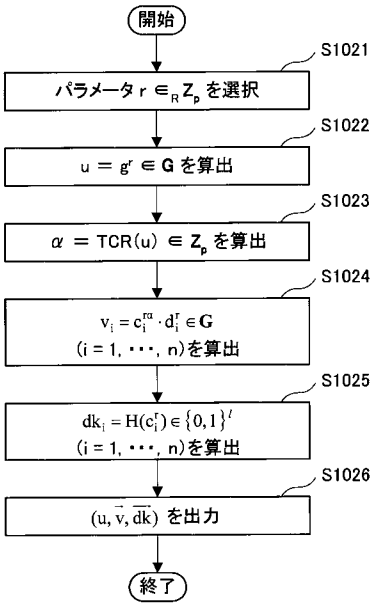
【図１７】



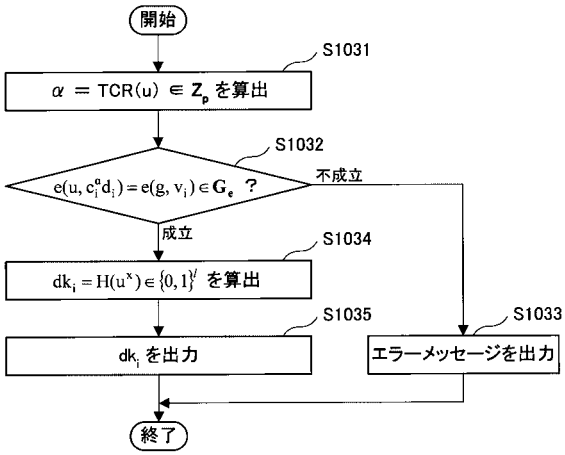

【図１８】



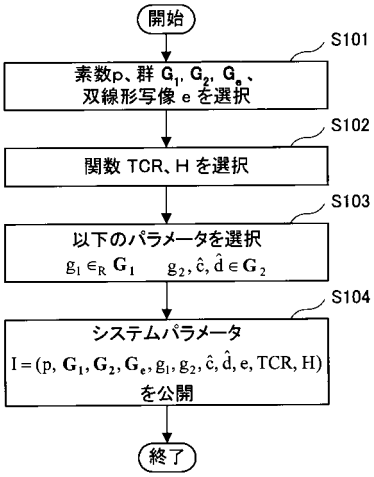

【図１９】



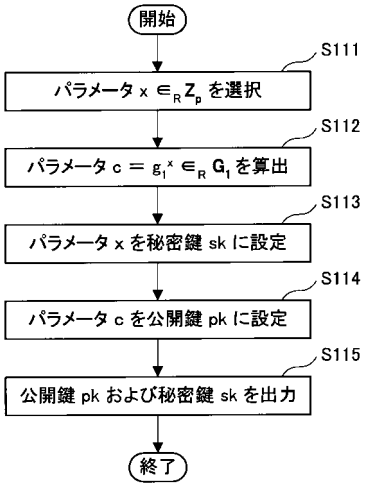

【図２０】



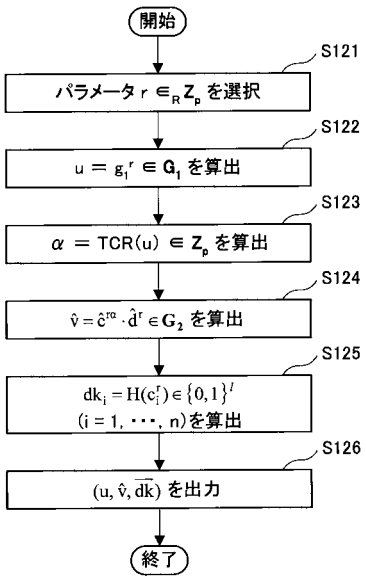
【図２１】



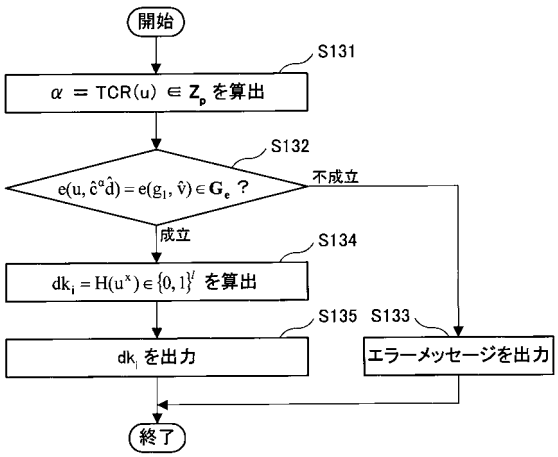

【図２２】



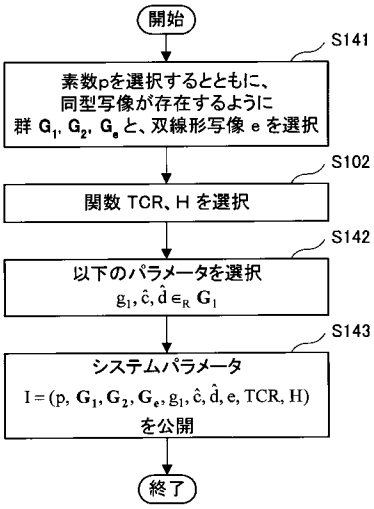

【図２３】



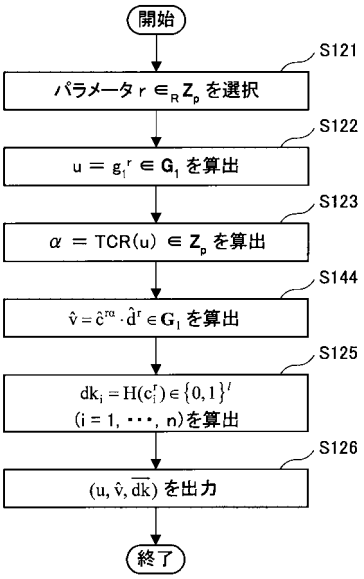

【図２４】



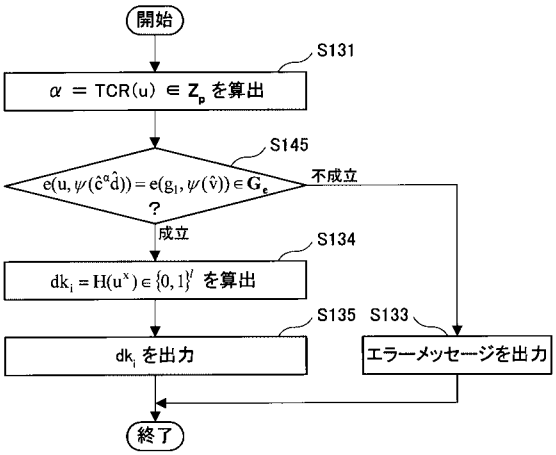
【図２５】



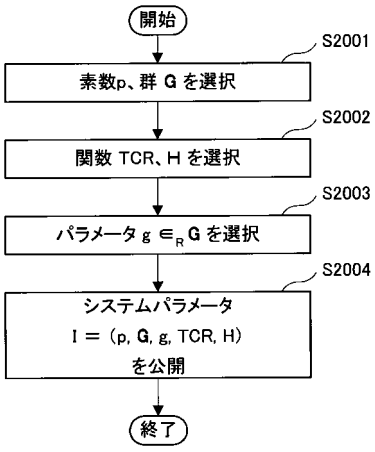

【図２６】



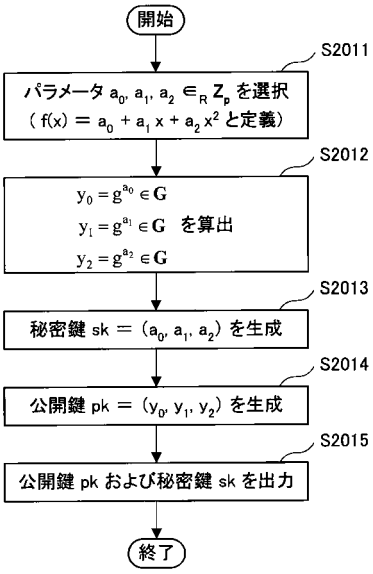

【図２７】



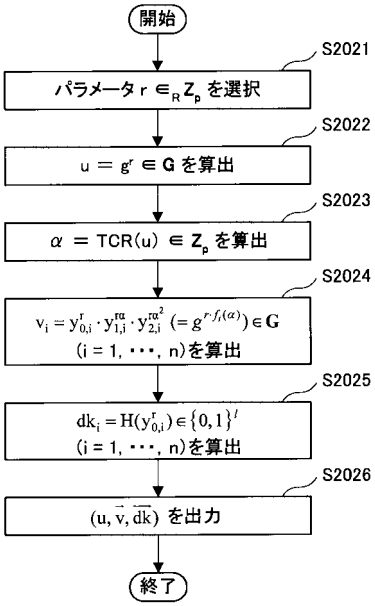

【図２８】



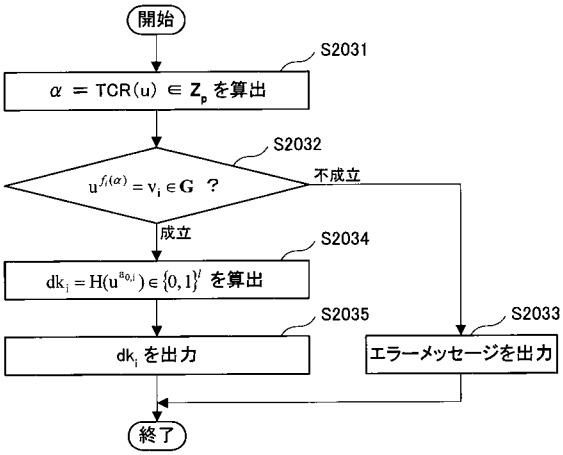
【図２９】



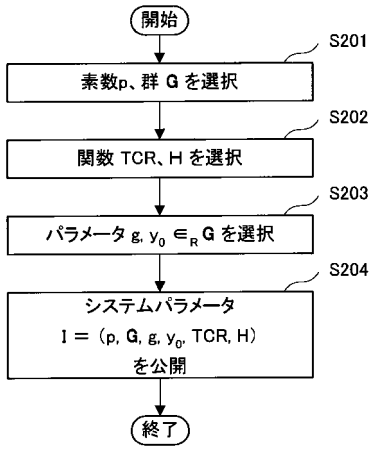

【図３０】



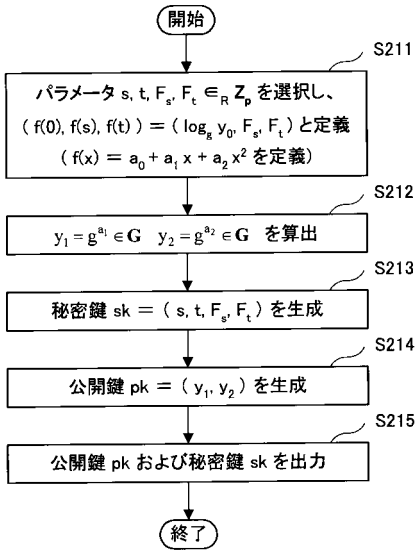

【図３１】



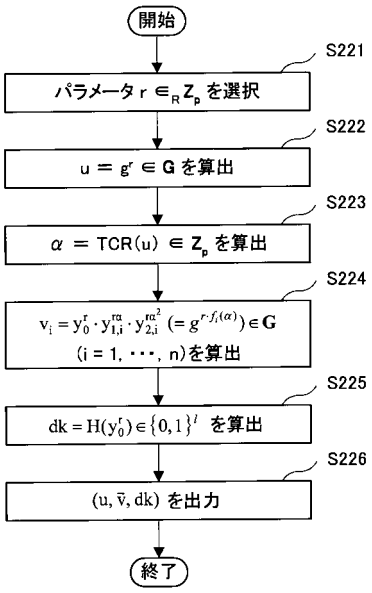

【図３２】



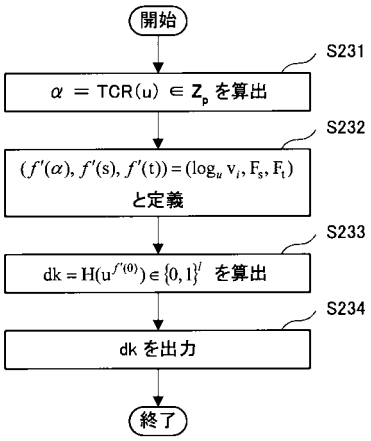
【図３３】



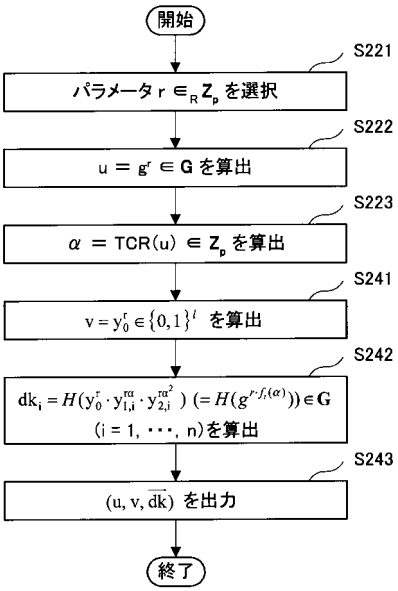

【図３４】



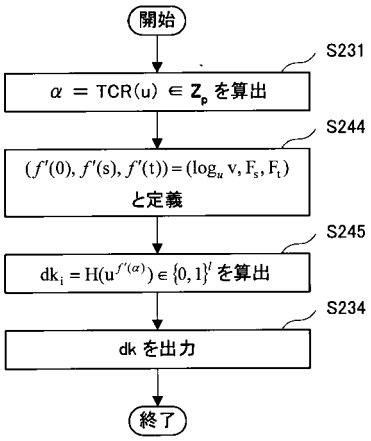

【図３５】



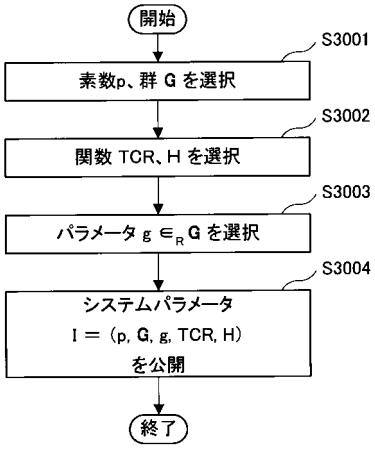

【図３６】



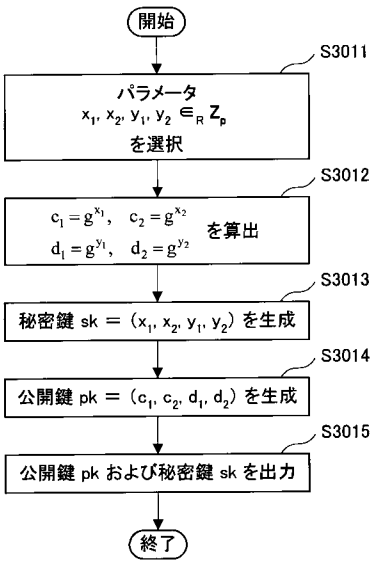
【図３７】



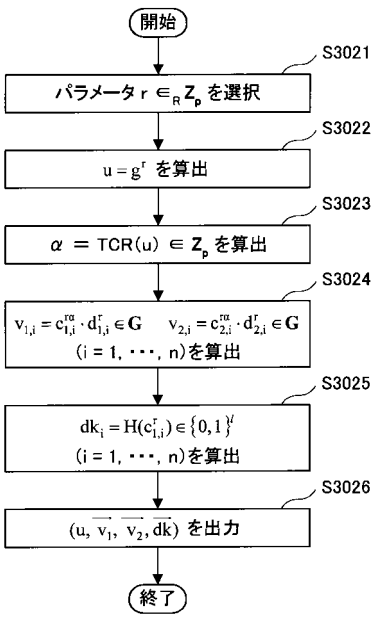

【図３８】



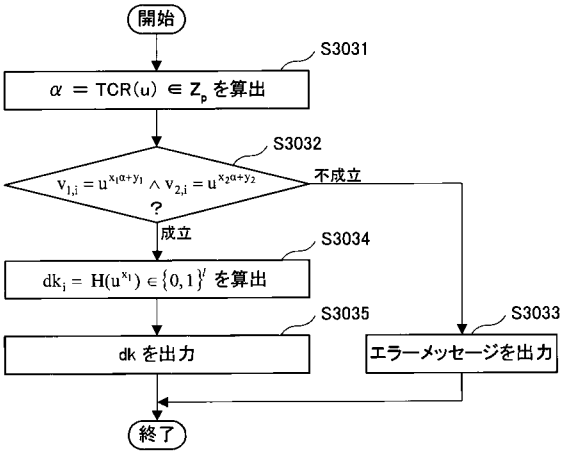

【図３９】



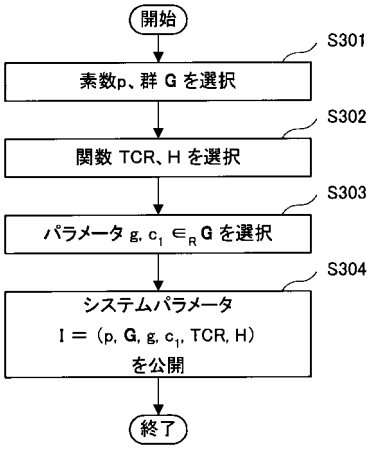

【図４０】



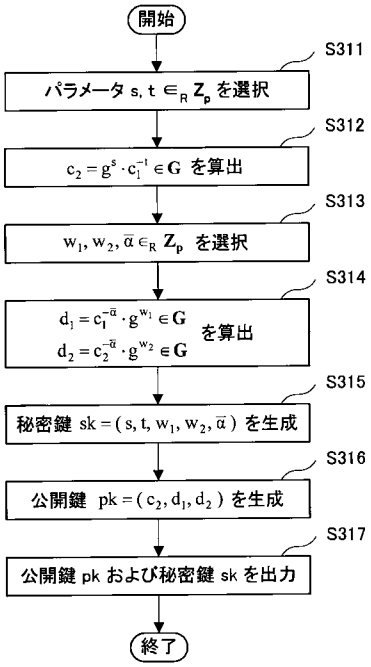
【図４１】



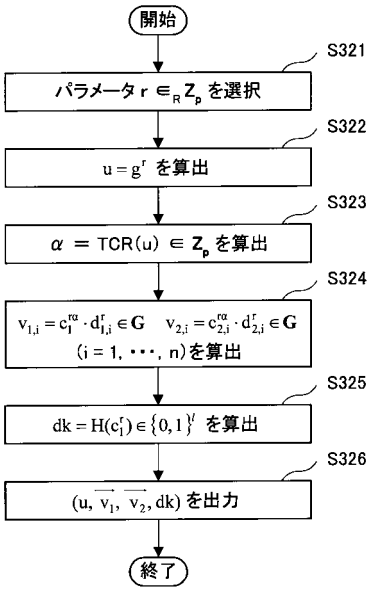

【図４２】



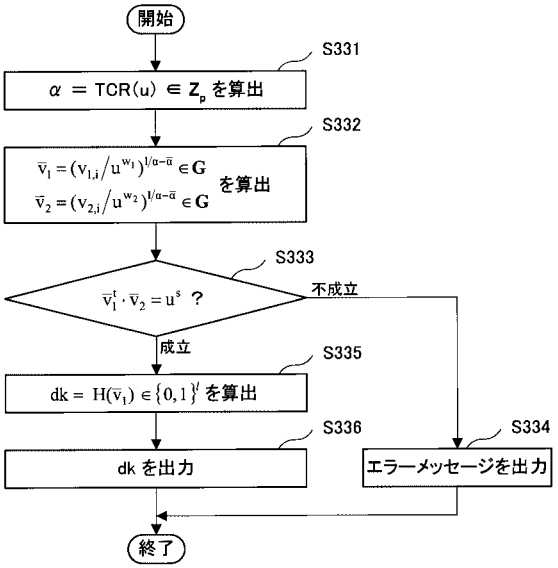

【図４３】



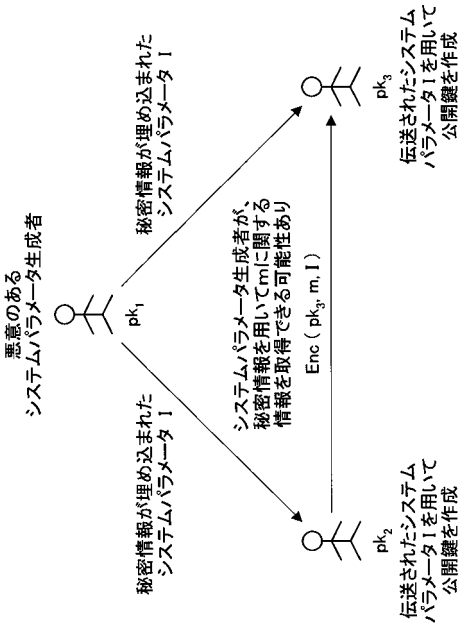

【図４４】



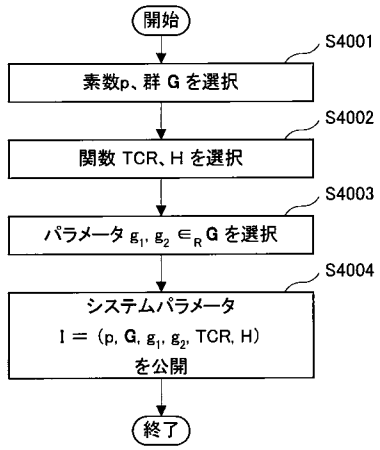
【図４５】



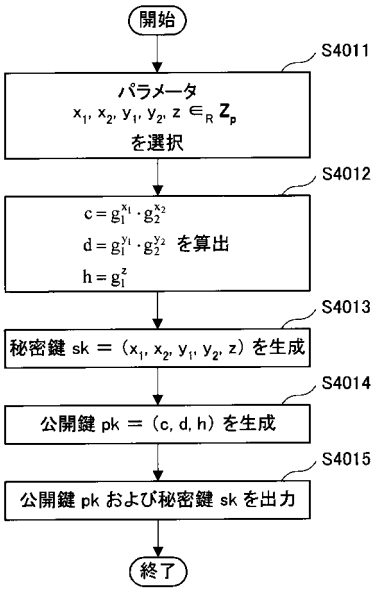

【図４６】



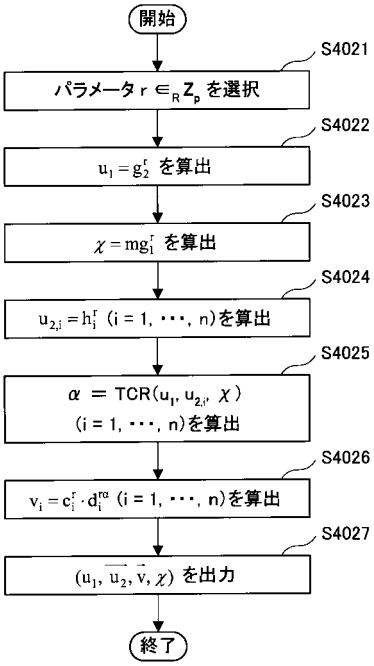

【図４７】



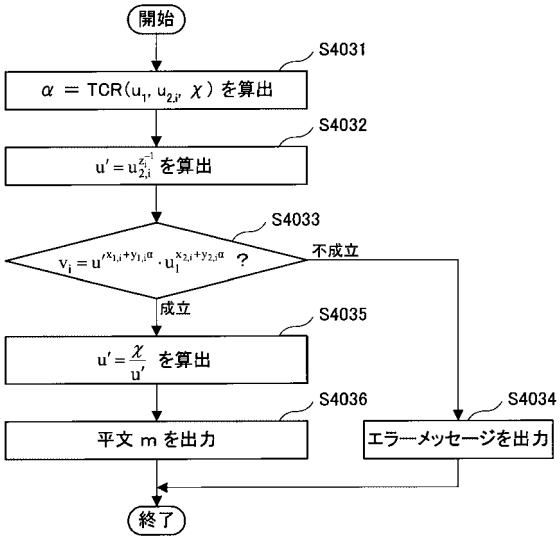

【図４８】



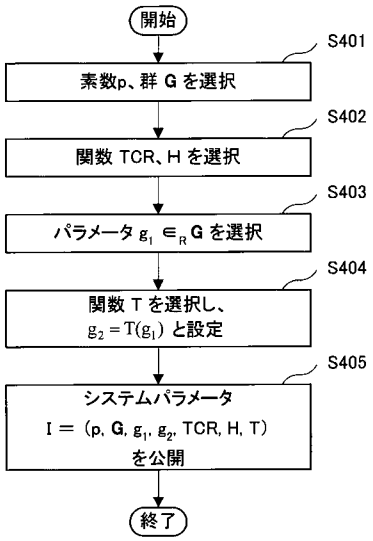
【図４９】



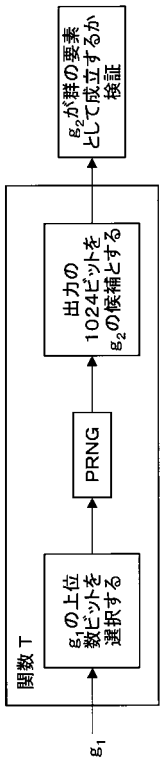

【図５０】



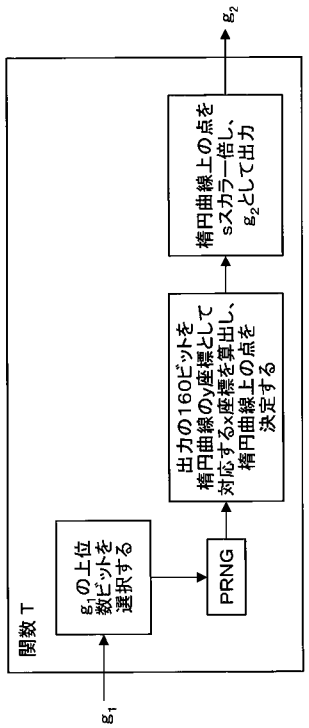

【図５１】



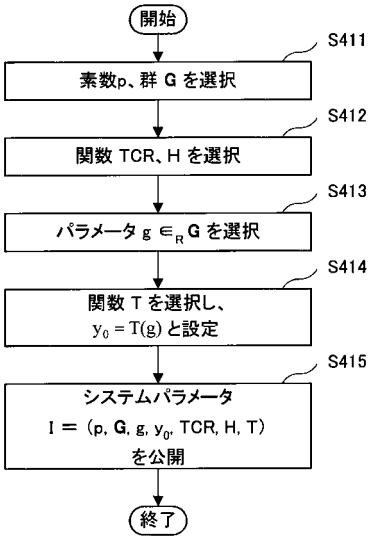

【図５２】



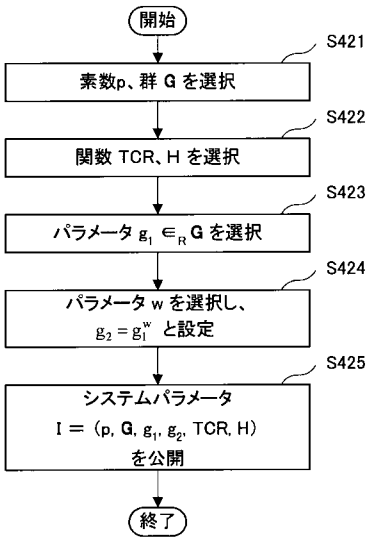
【図５３】



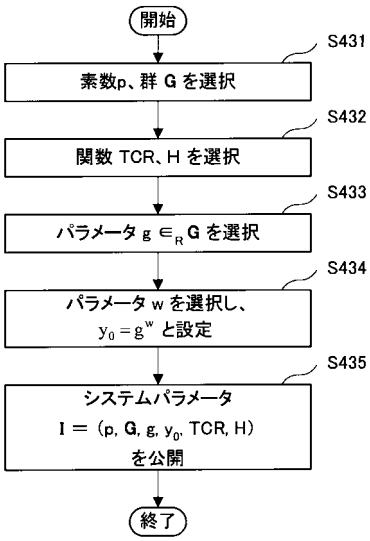

【図５４】



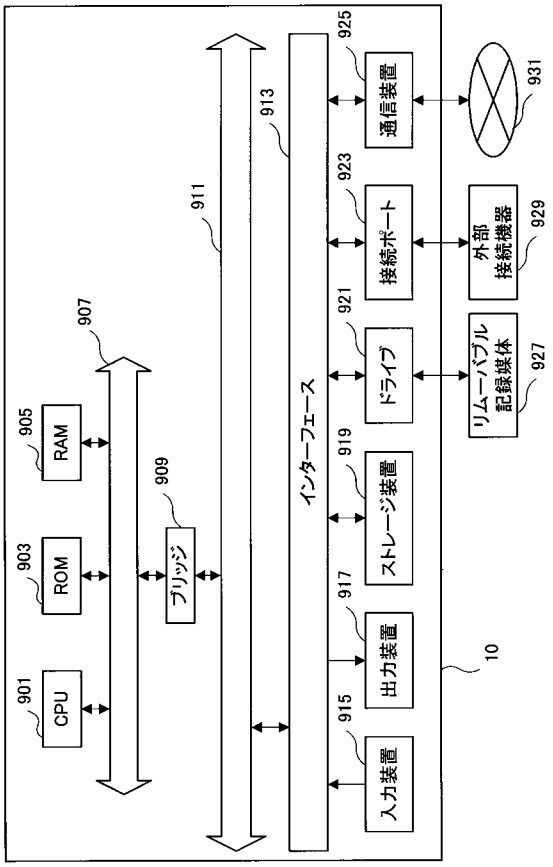

【図５５】




【図５６】



【図５７】


CPU
901
ROM
903
RAM
905
ブリッジ
909
907
911
913
インターフェース
入力装置
915
出力装置
917
ストレージ装置
919
ドライブ
921
接続ポート
923
通信装置
925
リムーバブル記録媒体
927
外部接続機器
929
931
10

フロントページの続き

(72)発明者　浅野　智之
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　作本　紘一
東京都港区港南１丁目７番１号　ソニー株式会社内

Ｆターム(参考) 5J104 AA16 AA18 AA32 EA01 EA04 EA08 EA18 EA19 FA00 JA03
JA21 MA05 NA02 NA03 NA37